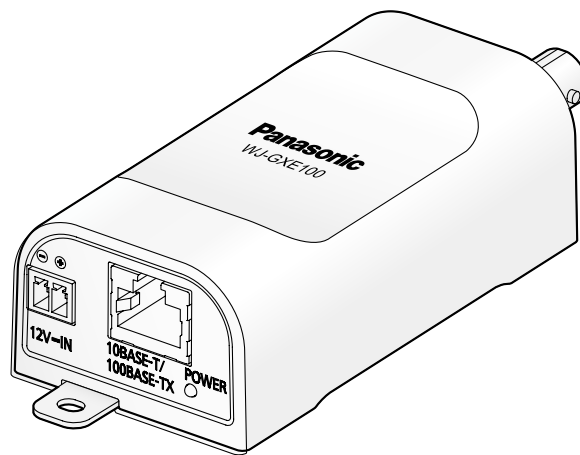


Panasonic

Operating Instructions

Network Video Encoder

Model No. WJ-GXE100
WJ-GXE100E



Before attempting to connect or operate this product, please read these instructions carefully and save this manual for future use.

The model number is abbreviated in some descriptions in this manual.

Preface

About the user manuals

There are 2 sets of operating instructions for the WJ-GXE100 (P model), WJ-GXE100E (E model) as follows.

- Installation Guide: Explains how to install and connect devices.
- Operating Instructions: Explains how to perform the settings and how to operate this unit.

The model number is abbreviated in some descriptions in this manual.

The screens used in these operating instructions show the case of WJ-GXE100 (P model). Depending on the model used, the screens shown in the explanations may differ to the actual unit screens.

Trademarks and registered trademarks

- Microsoft, Windows, Windows Vista, Internet Explorer, ActiveX and DirectX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.
- iPad, iPhone, and iPod touch are trademarks of Apple Inc., registered in the U.S. and other countries.
- Android is a trademark of Google Inc.
- Firefox is a registered trademark of the Mozilla Foundation.
- All other trademarks identified herein are the property of their respective owners.

Abbreviations

The following abbreviations are used in these operating instructions.

Microsoft® Windows® 7 is described as Windows 7.

Microsoft® Windows Vista® is described as Windows Vista.

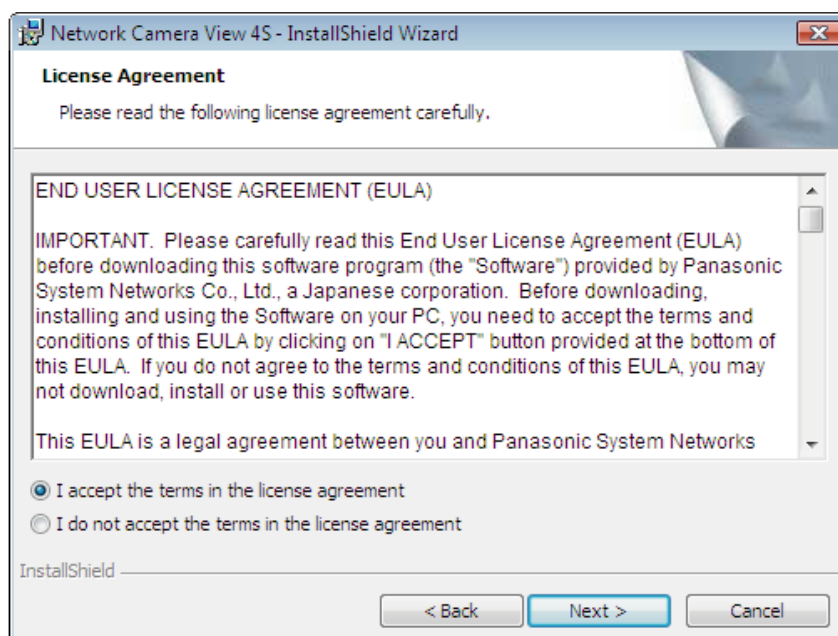
Microsoft® Windows® XP SP3 is described as Windows XP.

Windows® Internet Explorer® 9.0, Windows® Internet Explorer® 8.0, Windows® Internet Explorer® 7.0 and Microsoft® Internet Explorer® 6.0 are described as Internet Explorer.

Universal Plug and Play is described as UPnP™.

Viewer software

It is necessary to install the viewer software “Network Camera View 4S” (ActiveX®) to display images on a PC. This software can be installed directly from the unit or by selecting the [Install] button next to [Viewer Software] on the menu of the CD-ROM provided, and then following the on-screen instructions.



IMPORTANT

- The default setting of “Automatic installation of viewer software” is “On”. Follow the instructions on page 130 when the message is displayed on the information bar of the browser.
- When the “Live” page is displayed for the first time, the install wizard of the ActiveX control required to display images from the camera will be displayed. Follow the instructions of the wizard.
- When the install wizard is displayed again even after completing the installation of the ActiveX, restart the PC.
- The viewer software used on each PC should be licensed individually. The number of installations of the viewer software from the unit can be checked on the [Upgrade] tab of the “Maintenance” page (→page 106). Refer to your dealer for the software licensing.

Table of Contents

| | | |
|-----------|---|-----------|
| 1 | Monitor images on a PC | 7 |
| 1.1 | Monitor images from a single camera | 7 |
| 1.2 | About the “Live” page | 9 |
| 1.3 | Monitor images from multiple cameras | 13 |
| 2 | Monitor images on a cellular phone/mobile terminal | 14 |
| 2.1 | Monitor images on a cellular phone | 14 |
| 2.2 | Monitor images on a mobile terminal | 15 |
| 3 | Action at an alarm occurrence | 18 |
| 3.1 | Alarm type | 18 |
| 3.2 | Action at an alarm occurrence | 18 |
| 4 | Transmit images onto an FTP server | 19 |
| 4.1 | Transmit an alarm image at an alarm occurrence (Alarm image transmission) | 19 |
| 4.2 | Transmit images at a designated interval or period (FTP periodic image transmission) | 19 |
| 5 | About the network security | 20 |
| 5.1 | Equipped security functions | 20 |
| 6 | Display the setup menu from a PC | 21 |
| 6.1 | How to display the setup menu | 21 |
| 6.2 | How to operate the setup menu | 23 |
| 6.3 | About the setup menu window | 25 |
| 7 | Configure the basic settings of the unit [Basic] | 27 |
| 7.1 | Configure the basic settings [Basic] | 27 |
| 7.2 | Configure the Internet settings [Internet] | 30 |
| 8 | Configure the settings relating to images [Image] | 32 |
| 8.1 | Configure the settings relating to the Picture (Camera) mode/Video input [JPEG/H. 264] | 32 |
| 8.2 | Configure the settings relating to JPEG images [JPEG/H.264] | 33 |
| 8.3 | Configure the settings relating to H.264 images [JPEG/H.264] | 35 |
| 8.4 | Configure the settings relating to image and positions [Image/Position] | 40 |
| 8.5 | Configure the settings relating to RS485 [RS485] | 41 |
| 9 | Configure the multi-screen settings [Multi-screen] | 44 |
| 10 | Configure the alarm settings [Alarm] | 46 |
| 10.1 | Configure the settings relating to the alarm action [Alarm] | 46 |
| 10.2 | Configure the settings relating to the alarm image [Alarm] | 47 |
| 10.3 | Configure the VMD settings [VMD area] | 48 |
| 10.3.1 | Set the VMD areas [VMD area] | 50 |
| 10.4 | Configuration of the settings relating to the E-mail notification [Notification] | 52 |
| 10.5 | Configure the settings relating to Panasonic alarm protocol [Notification] | 53 |
| 11 | Configure the settings relating to the authentication [User mng.] | 56 |
| 11.1 | Configure the settings relating to the user authentication [User auth.] | 56 |

| | | |
|-----------|--|------------|
| 11.2 | Configure the settings relating to the host authentication [Host auth.] | 57 |
| 11.3 | Configure the settings relating to the priority stream [System] | 58 |
| 12 | Configure the settings of the servers [Server] | 61 |
| 12.1 | Configure the settings relating to the E-mail server [E-mail] | 61 |
| 12.2 | Configure the settings relating to the FTP server [FTP] | 62 |
| 12.3 | Configure the settings relating to the NTP server [NTP] | 64 |
| 13 | Configuring the network settings [Network] | 66 |
| 13.1 | Configure the network settings [Network] | 66 |
| 13.2 | Configure the HTTPS settings | 74 |
| 13.2.1 | Generation of the CRT key (SSL encryption key) | 75 |
| 13.2.2 | Generation of the self-signed certificate (security certificate) | 76 |
| 13.2.3 | Generation of CSR (Certificate Signing Request) | 78 |
| 13.2.4 | Installation of the server certificate | 79 |
| 13.2.5 | Configuration of the connection protocol | 80 |
| 13.3 | Access the unit using the HTTPS protocol | 81 |
| 13.3.1 | Install the security certificate | 81 |
| 13.4 | Configure the settings relating to DDNS [DDNS] | 91 |
| 13.4.1 | Configuration of the DDNS service (Example of the "Viewnetcam.com" service) | 92 |
| 13.4.2 | When using the "Viewnetcam.com" service | 93 |
| 13.4.3 | Procedure to register information for the "Viewnetcam.com" service | 94 |
| 13.4.4 | Checking the information registered for the "Viewnetcam.com" service | 97 |
| 13.4.5 | When using "Dynamic DNS Update" | 97 |
| 13.4.6 | When using "Dynamic DNS Update(DHCP)" | 97 |
| 13.5 | Configure the settings relating to SNMP [SNMP] | 98 |
| 13.6 | Configure the settings relating to the FTP periodic image transmission [FTP img. trans.] | 99 |
| 13.7 | Configure the schedule settings of the FTP periodic image transmission [FTP img. trans.] | 100 |
| 13.7.1 | How to set the schedules | 101 |
| 13.7.2 | How to delete the set schedule | 102 |
| 14 | Configure the settings relating to the schedules [Schedule] | 103 |
| 15 | Maintenance of the unit [Maintenance] | 106 |
| 15.1 | Check the system log [System log] | 106 |
| 15.2 | Upgrade the firmware [Upgrade] | 106 |
| 15.3 | Check the status [Status] | 108 |
| 15.4 | Reset the settings/Reboot the unit [Default reset] | 109 |
| 16 | Functional restrictions | 111 |
| 16.1 | Functional restrictions when "D1" is selected | 111 |
| 17 | Number of users that can concurrently access the unit | 112 |
| 18 | Using the CD-ROM | 113 |
| 18.1 | About the CD launcher | 113 |
| 18.2 | Installing Panasonic "IP Setting Software" | 114 |
| 18.3 | Installing the manuals | 115 |
| 18.4 | Installing the Viewer software | 115 |
| 18.5 | Configure the network settings of the unit using the Panasonic "IP Setting Software" | 116 |
| 19 | About the displayed system log | 118 |

20 Troubleshooting122

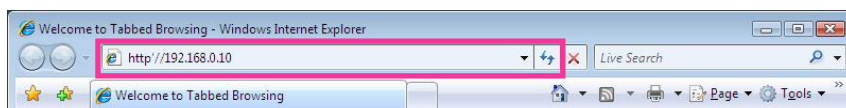
1 Monitor images on a PC

The following are descriptions of how to monitor images from the camera on a PC.

1.1 Monitor images from a single camera

1. Start up the web browser.
2. Enter the IP address designated using the Panasonic “IP Setting Software” in the address box of the browser.
 - **Example when entering an IPv4 address:** http://URL registered using IPv4 address
http://192.168.0.10/
 - **Example when entering an IPv6 address:** http://[URL registered using IPv6 address]
http://[2001:db8::10]/

<Example of IPv4 access>



<Example of IPv6 access>



IMPORTANT

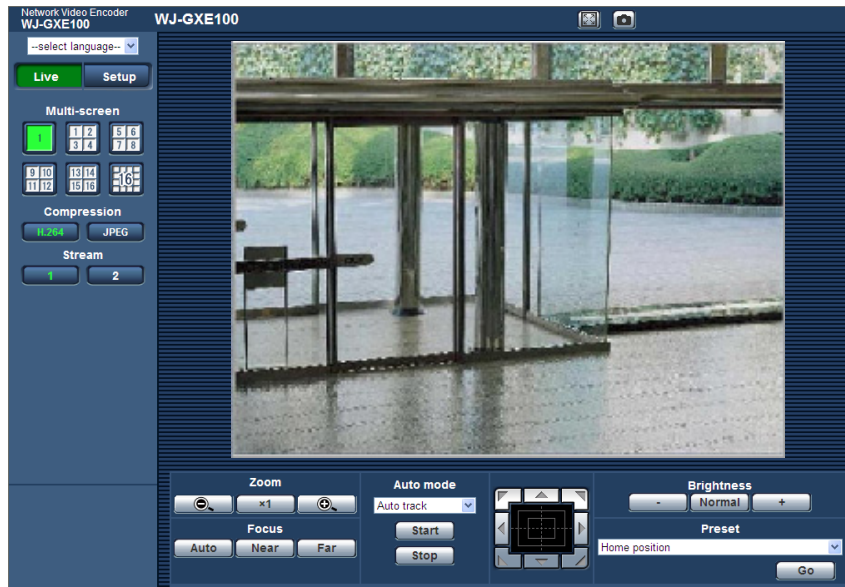
- When the HTTP port number is changed from “80”, enter “http://IP address of the unit + : (colon) + port number” in the address box of the browser. (Example: http://192.168.0.11:8080)
- When the PC is in a local network, configure the proxy server setting of the web browser (under [Internet Options...] under [Tools] of the menu bar) to bypass the proxy server for the local address.

Note

- Refer to page 81 for further information about the case in which “HTTPS” is selected for “HTTPS” - “Connection” on the [Network] tab of the “Network” page (→page 66).

3. Press the [Enter] key on the keyboard.

→ The “Live” page will be displayed. Refer to page 9 for further information about the “Live” page.



When “On” is selected for “User auth.”, the authentication window will be displayed before displaying live images for the user name and password entries. The default user name and password are as follows.

User name: admin

Password: 12345

IMPORTANT

- To enhance the security, change the password for the user name “admin”. It is recommended to change this password periodically.
- When displaying multiple H.264 images on a PC, images may not be displayed depending on the performance of the PC.

Note

- The maximum number of concurrent access user is 14 including users who is receiving H.264 images and users who are receiving JPEG images. Depending on the set values for “Bandwidth control(bit rate)” and “Max bit rate (per client)”, the maximum concurrent access number may be 14 or less users. When 14 users are concurrently accessing, the access limit message will be displayed for users who subsequently attempt to access. When “Multicast” is selected for “Transmission type” of “H.264”, only the first user who accessed to monitor H.264 images will be included in the maximum number. The second and subsequent users who are monitoring H.264 images will not be included in the maximum number.
- When “On” is selected for “H.264 transmission” (→page 36), H.264 images will be displayed. When “Off” is selected, a JPEG image will be displayed. It is possible to display a JPEG image even when “On” is selected for “H.264 transmission”. In this case, the refresh interval of JPEG images will be limited.
- The refresh interval may become longer depending on a network environment, PC performance, photographic subject, access traffic, etc.

<Refresh interval of JPEG images>

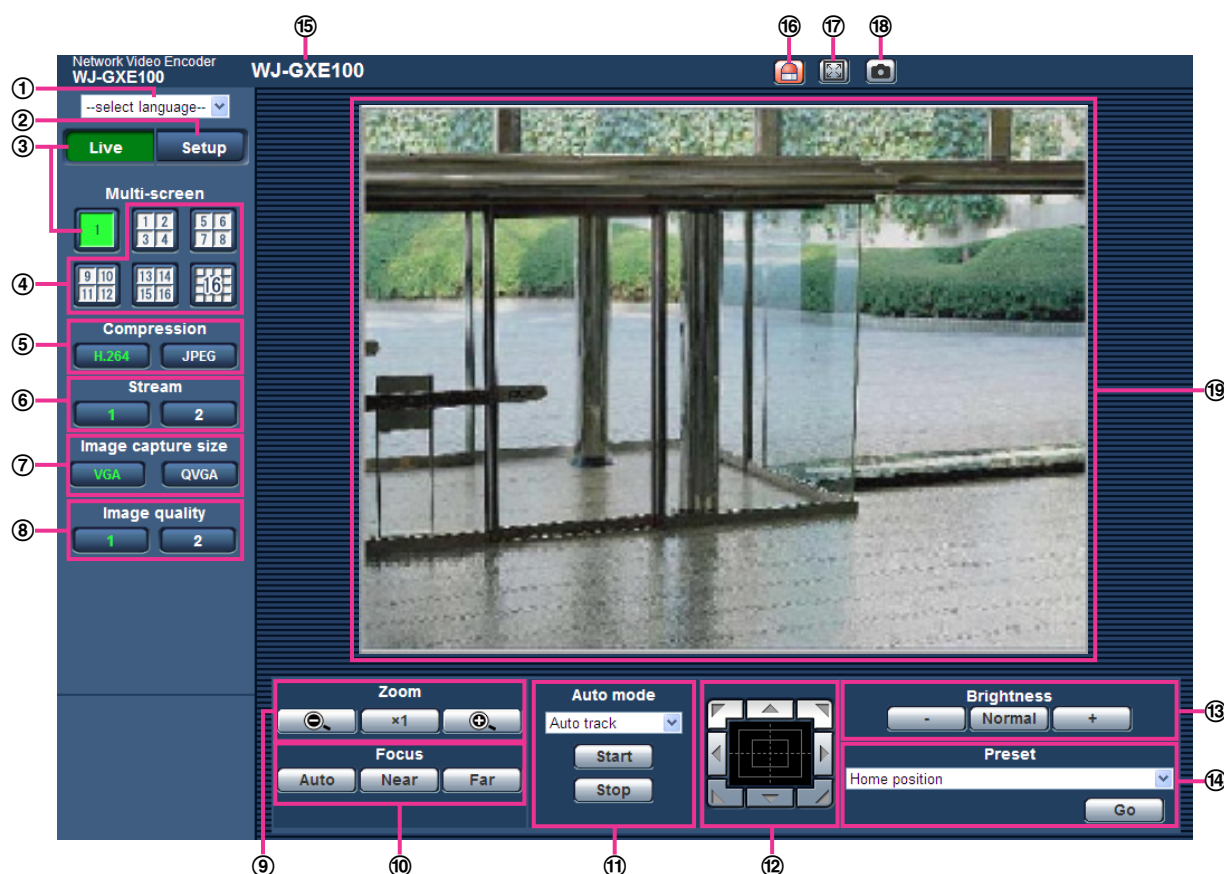
When “On” is selected for “H.264 transmission”

NTSC: Max. 5 fps, PAL: Max. 4.2 fps

When “Off” is selected for “H.264 transmission”

NTSC: Max. 30 fps, PAL: Max. 25 fps

1.2 About the “Live” page



① [select language] pull-down-menu

The unit's display language can be selected. The default language can be set in the [Language] in the [Basic] settings. (→page 27)

② [Setup] button¹⁾

Displays the setup menu. The button will turn green and the setup menu will be displayed.

③ [Live] button

Displays the “Live” page. The button will turn green and the “Live” page will be displayed.

④ [Multi-screen] buttons

Images from multiple cameras can be displayed on a multi-screen by registering units/network cameras on the setup menu. (→page 13)

⑤ [Compression] buttons

- **[H.264] button:** The characters “H.264” on the button will turn green and an H.264 image will be displayed. When “On” is selected for “H.264 transmission” of “H.264(1)”, “H.264(2)”, the [H.264] button will be displayed. (→page 36)
- **[JPEG] button:** The characters “JPEG” on the button will turn green and a JPEG image will be displayed.

⑥ [Stream] buttons

These buttons will be displayed only when an H.264 image is displayed.

- **[1] button:** The character “1” will turn green and images in the main area will be displayed in accordance with the setting of “H.264(1)”. (→page 36)
- **[2] button:** The character “2” will turn green and images in the main area will be displayed in accordance with the setting of “H.264(2)”. (→page 36)

⑦ [Image capture size] buttons

These buttons will be displayed only when a JPEG image is displayed.

| | |
|------------------|--|
| [VGA] | The characters "VGA" will turn green and images in the main area will be displayed in VGA size. |
| [QVGA] | The characters "QVGA" will turn green and images in the main area will be displayed in QVGA size. |
| [640x360] | The characters "640x360" will turn green and images in the main area will be displayed in 640x360 (pixels). |
| [320x180] | The characters "320x180" will turn green and images in the main area will be displayed in 320x180 (pixels). |
| [D1] | The characters "D1" will turn green and images in the main area will be displayed in D1 (NTSC: 720x480 pixels, PAL: 720x576 pixels). |

Note




- The buttons [VGA] and [QVGA] are displayed only when "VGA [4:3]" is selected for "Picture (Camera) mode".
- The buttons [640x360] and [320x180] are displayed only when "VGA [16:9]" is selected for "Picture (Camera) mode".
- The [D1] button will be displayed only when "D1" is selected for "Picture (Camera) mode".

⑧ [Image quality] buttons

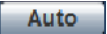
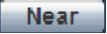
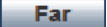
These buttons will be displayed only when a JPEG image is displayed.

- **[1] button:** Images in the main area will be displayed in accordance with the setting for "Quality1" of "Image quality setting". (→page 33)
- **[2] button:** Images in the main area will be displayed in accordance with the setting for "Quality2" of "Image quality setting". (→page 33)

⑨ [Zoom] buttons²

- : Click this button to adjust the zoom ratio to the "Wide" side.
- : Click this button to set the zoom ratio to x1.0.
- : Click this button to adjust the zoom ratio to the "Tele" side.

⑩ [Focus] buttons²

- : Click this button to adjust the focus automatically.
- : Click this button to adjust the focus to the "Near" side.
- : Click this button to adjust the focus to the "Far" side.

⑪ [Auto mode]²

Select an operation from the pull-down menu and click the [Start] button. The selected operation will start. Click the [Stop] button to stop the operation.

The selected operation will stop when the camera (panning/tilting/zooming/focusing) is operated.

- **Auto track:** Automatically performs tracking for cameras that supports auto track.
- **Auto pan:** Automatically pans between the start position and the end position set in advance. Even when the camera is operated for zooming or focusing, the camera continues panning. (However, panning will stop when the zoom button (x1) is clicked.)
- **Preset sequence:** Automatically moves to the preset positions orderly (start from the lowest preset position number).
- **Patrol 1-4:** Performs patrols 1-4 that were set in advance.

Note

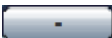
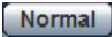

- To check if the camera supports auto track, refer to the operating instructions of the camera.

- While a camera controlled via RS485 communication is executing a patrol function, it is impossible to start another one. Stop the current patrol function before starting a new one.
- To activate auto pan, sort, preset position sequence or patrol 1-4, it is required to perform the settings on the setup menu of camera in advance. (→page 40)

⑫ Control pad/buttons²

- Left-click on the control pad or buttons to adjust the horizontal/vertical position of the camera (panning/tilting). Panning/tilting speed will be faster if a clicked point gets farther from the center point of the control pad.
It is also possible to pan/tilt the camera by dragging the mouse.
Zoom and focus can be adjusted by right-clicking. When an upper/lower area of the control pad is right-clicked, the displayed image will be zoomed in/out on. When a left/right area is right-clicked, the focus will be adjusted to the Near/Far side.
Zoom can also be adjusted using the mouse wheel.

⑬ [Brightness] buttons²

-  button: Image become darker.
-  button: The adjusted brightness will return to the default brightness.
-  button: Image become brighter.

⑭ [Preset]²

Select a preset position from the pull-down menu and click the [Go] button. The camera will move to the selected preset position. When "Home position" is selected, the camera will move to the home position. Preset positions and the home position can be registered in the camera's setup menu. (→page 40)

⑮ Unit title

The title entered for "Unit title" on the [Basic] tab will be displayed. (→page 27)

⑯ Alarm occurrence indication button²

This button will be displayed and will blink when an alarm has occurred. When this button is clicked, this button will disappear. (→page 18)

⑰ Full screen button

Images will be displayed on a full screen. To return to the "Live" page, press the [Esc] key. The aspect ratio of displayed images will be adjusted in accordance with the monitor.

⑱ Snap shot button

Click this button to take a picture (a still picture). The picture will be displayed on a newly opened window. When right-clicking on the displayed image, the pop-up menu will be displayed. It is possible to save the image on the PC by selecting "Save" from the displayed pop-up menu. When "Print" is selected, printer output is enabled.

Note

- For the case of using Windows 7 or Windows Vista, the following settings may be required. Open Internet Explorer, click [Tools] → [Internet Options] → [Security] → [Trusted Sites] → [Sites]. Register the unit address on [Website] of the displayed trusted widows.

⑲ Main area

Images from the camera will be displayed in this area.

The current time and date will be displayed according to the settings configured for "Time display format" and "Date/time display format". (→page 27)

When clicking a desired point while displaying live images in the main area, the camera will move to locate the clicked point at the center of the main area.

Note

- When operated by a lower access level user, images displayed on the screen may be changed temporarily. This does not affect operation of the unit.
- Depending on the PC in use, screen tearing* may occur when the shooting scene drastically changes due to the GDI restrictions of the OS.

1 Monitor images on a PC

*A phenomenon in which portions of the screen are displayed out of alignment.

*1 Only operable by users whose access level is "1. Administrator".

*2 Only operable by users whose access level is "1. Administrator" or "2. Camera control" when "On" is selected for "User auth."
(→page 56)

1.3 Monitor images from multiple cameras

Images from multiple cameras can be displayed on a multi-screen. Images from 4 cameras (up to 16 cameras) can be displayed simultaneously. In order to use multi-screen, IP addresses of network cameras and units used to connect to cameras must be configured to the unit. 4 cameras can be registered as a group and up to 4 groups (16 cameras) can be registered. (→page 44)

IMPORTANT

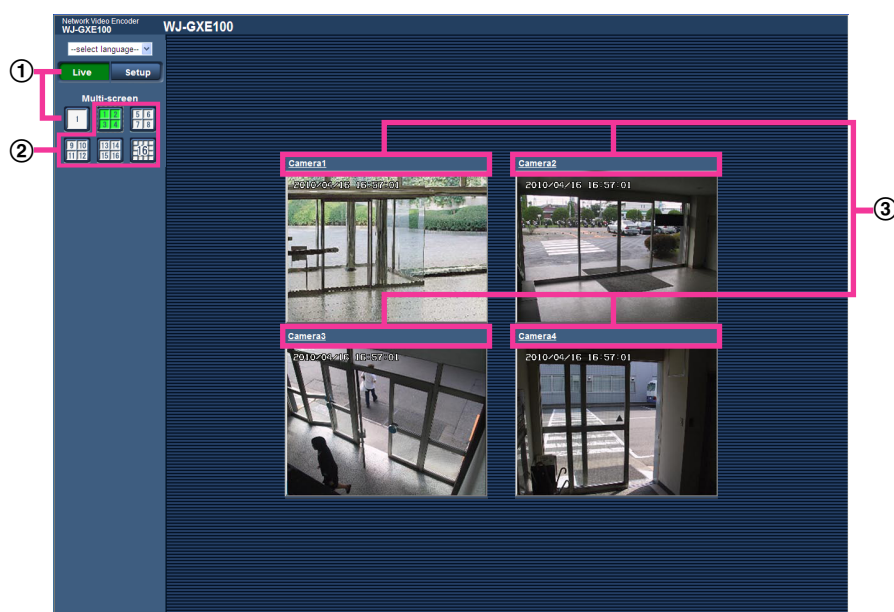
- When displaying images on a 16-screen, panning, tilting and zooming operations become unavailable for images from cameras with Pan/Tilt/Zoom functions.
- When the power is turned off or the LAN cable is disconnected while displaying images, displaying images on a multi-screen from the “Live” page will become unavailable.

Note

- When displaying images on a 4-screen, panning, tilting and zooming operations become available only for images from cameras with Pan/Tilt/Zoom functions. Refer to our website (<http://panasonic.net/pss/security/support/info.html>) for further information about the compatible cameras and their versions.
- Only JPEG images can be displayed on a multi-screen.
- When displaying images on multi-screen from cameras that have the aspect ratio configured to a setting other than “4:3”, the image will be displayed altered to the aspect ratio of “4:3”.
- “Network Camera Recorder with Viewer Software Lite” which supports live monitoring and recording images from multiple cameras is available. For further information, refer to our website (<http://panasonic.net/pss/security/support/info.html>).

1. Click the desired [Multi-screen] button.

→ Images from the registered cameras will be displayed on a selected multi-screen (screen can be split up to 16 areas). The following are instructions when displaying on a 4-split screen.



- ① To show 1 camera screen, click the [Live] button.
You can also click “1” below “Multi-screen” to display the live image from the camera.
- ② Click the [Multi-screen] button to display images from cameras in a multi-screen of 4 to 16 screens.
- ③ Click a camera title. Live images from the camera corresponding to the clicked camera title will be displayed on the “Live” page of the newly opened window.

2 Monitor images on a cellular phone/mobile terminal

2.1 Monitor images on a cellular phone

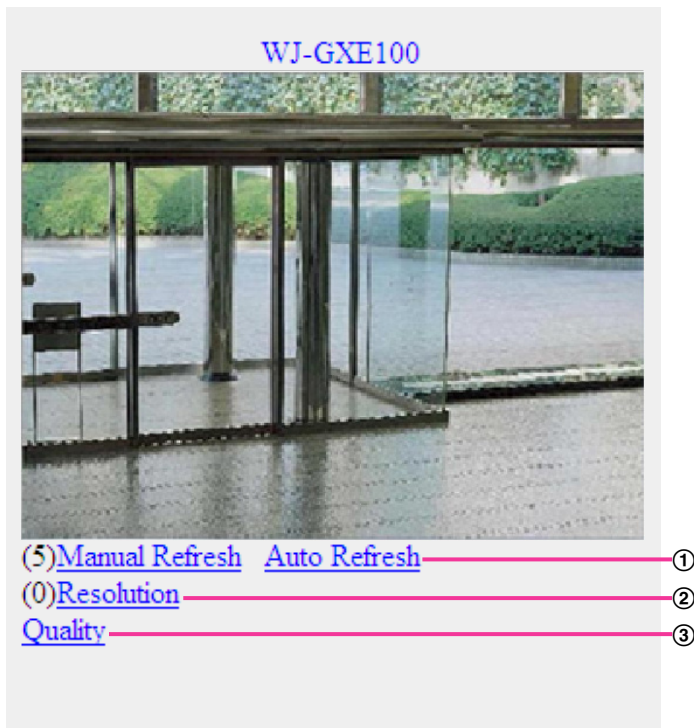
It is possible to connect to the unit using a cellular phone via the Internet and monitor images (JPEG only) from the unit on the screen of the cellular phone. It is also possible to refresh images to display the latest image.

IMPORTANT

- When the authentication window is displayed, enter the user name and password. The default user name and password are as follows.
User name: admin
Password: 12345
To enhance the security, change the password for the user “admin”. (→page 56)
- If the cellular phone in use is not compatible with UTF-8 encode, it is impossible to display the screen correctly.

Note

- It is necessary to configure the network settings of the cellular phone in advance to connect to the Internet and monitor images from the unit. (→page 66)
1. Access to “http://IP address/mobile”¹ or “http://Host name registered in the DDNS server/mobile” using a cellular phone.
→ Images from the unit will be displayed.



- ① Manual Refresh/Auto Refresh
Press the dial key “5” or the [Manual Refresh] button to refresh the camera images.
Press the [Auto Refresh] button to refresh the images from the camera in 5-second intervals.

When the dial key “5” or the [Manual Refresh] button is pressed again, the refresh mode of the camera will return to manual refresh.

IMPORTANT

- Transmission will be periodically performed when “Auto Refresh” is selected for the camera image. Confirm the contract plan of the cellular phone in use before using this function.
- Depending on the cellular phone in use, “Auto Refresh” may be unavailable.

② Resolution control

Changes the image capture size by pressing the dial key “0”.

When “D1” is selected for “Picture (Camera) mode”, “Resolution” will not be displayed.

| | |
|----------------------------------|---------------------------|
| Picture (Camera) mode VGA [4:3] | 320x240 (default)/640x480 |
| Picture (Camera) mode VGA [16:9] | 320x180 (default)/640x360 |

③ Image quality control

It is possible to change the image quality between “Quality1” and “Quality2”. (→page 33)

Note

- The pan/tilt/zoom/focus functions of cameras connected to the unit cannot be operated from cellular phones.
- Some cellular phones cannot change the image capture size even when resolution is changed by resolution control.
- When the HTTP port number is changed from “80”, enter “http://IP address: (colon) + port number/mobile”^{*1} in the address box of the browser. When using the DDNS function, access to “http://Host name registered in the DDNS server: (colon) + port number/mobile”.
- When the authentication window is displayed, enter the user name of an administrator or user and password. Depending on the cellular phone in use, password entry may be required each time the screen is switched.
- Depending on the cellular phone in use, larger size images may not be displayed. In this case, selecting “9 Low” for “Image quality setting” of “JPEG” (→page 33) may sometimes solve this problem.
- Depending on the cellular phone in use or its contract plan, it may be impossible to access.
- When “HTTPS” is selected for “HTTPS” - “Connection” on the [Network] tab of the “Network” page, enter as follows.
“https://IP address: (colon) + port number/mobile” or “https://Host name registered in the DDNS server: (colon) + port number/mobile”

^{*1} IP address is the global WAN IP address of the router that can be accessed via the Internet.

2.2 Monitor images on a mobile terminal

It is possible to connect to the unit using a mobile terminal via the Internet and monitor images (MJPEG only) from the unit on the screen of the mobile terminal. Images are refreshed automatically to display the latest image.

The compatible mobile terminals are shown as follows. (As of December, 2012)

- iPad, iPhone, iPod touch (iOS 4.2.1 or later)
- Android™ mobile terminals

When an Android terminal is used, an MJPEG format image is displayed by the Firefox® browser, but a JPEG format image is displayed by the standard browser.

For further information about compatible devices, refer to our website

(<http://panasonic.net/pss/security/support/info.html>).

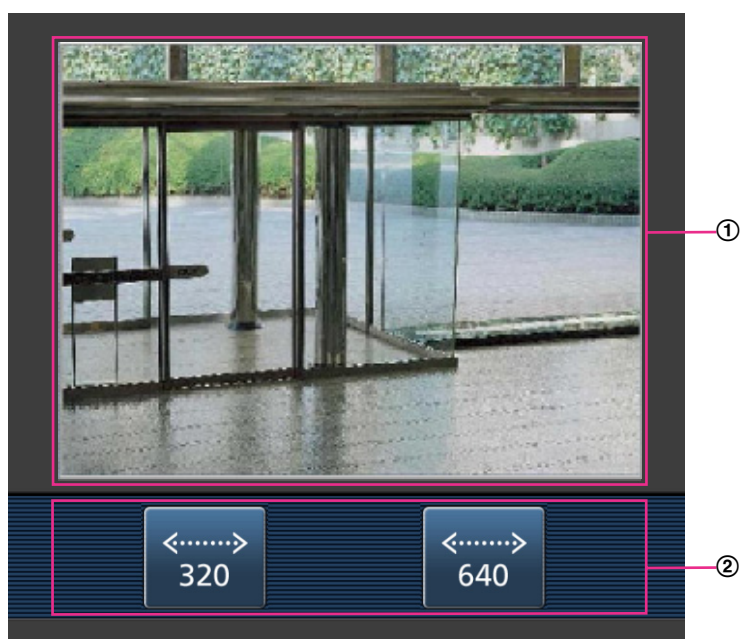
2 Monitor images on a cellular phone/mobile terminal

IMPORTANT

- When the authentication window is displayed, enter the user name and password. The default user name and password are as follows.
User name: admin
Password: 12345
To enhance the security, change the password for the user "admin". (→page 56)

Note

- It is necessary to configure the network settings of the mobile terminal in advance to connect to the Internet and monitor images from the unit. (→page 66)
- Access to "http://IP address/cam"¹ or "http://Host name registered in the DDNS server/cam"² using a mobile terminal.
→ Images from the unit will be displayed.



- ① Live images area
Displays images from the camera.
- ② Resolution control
The resolution can be changed by selecting a resolution setting from the buttons.
When "D1" is selected for "Picture (Camera) mode", the resolution control buttons will not be displayed.

| | |
|----------------------------------|---------------------------|
| Picture (Camera) mode VGA [4:3] | 320x240/640x480 (default) |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 (default) |

Note

- You can change the image size displayed on the mobile terminal by accessing the following addresses.
 - Large display: <http://IP address/cam/dl>
 - Medium display: <http://IP address/cam/dm>
 - Small display: <http://IP address/cam/ds>
- The pan/tilt/zoom/focus functions of cameras connected to the unit cannot be operated from mobile terminals.

- When the resolution is changed by the resolution control, the displayed resolution changes but the image size remains the same.
- When the HTTP port number is changed from “80”, enter “http://IP address: (colon) + port number/cam”^{*1} in the address box of the browser. When using the DDNS function, access to “http://Host name registered in the DDNS server: (colon) + port number/cam”^{*2}.
- When “HTTPS” is set in “HTTPS” - “Connection” on the [Network] tab of the “Network” page, enter the following:
“https://IP address: (colon) + port number/cam” or “https://Host name registered in the DDNS server: (colon) + port number/cam”.
- When the authentication window is displayed, enter the user name of an administrator or user and password. Depending on the mobile terminal in use, password entry may be required each time the screen is switched.
- Depending on the mobile terminal in use, larger size images may not be displayed. In this case, selecting “9 Low” for “Image quality setting” of “JPEG” (→page 33) may sometimes solve this problem.
- Depending on the mobile terminal in use or its contract plan, it may be impossible to access.

^{*1} IP address is the global WAN IP address of the router that can be accessed via the Internet. However, when accessing the same LAN as the unit with a wireless compatible mobile terminal, the IP address is the local IP address.

^{*2} Only when accessing the unit through the Internet.

3 Action at an alarm occurrence

The alarm action (action at an alarm occurrence) will be performed when the following alarms occur.

3.1 Alarm type

- **VMD alarm:** When motion is detected in the set VMD area, the alarm action will be performed.
*VMD stands for “Video Motion Detection”.
- **Command alarm:** When a Panasonic alarm protocol is received from the connected device via a network, the alarm action will be performed.
- **Video loss alarm:** The alarm will be activated when there is a loss of video input signals due to disconnection of the coaxial cable or camera problems.

3.2 Action at an alarm occurrence

Display the alarm occurrence indication button on the “Live” page

The alarm occurrence indication button will be displayed on the “Live” page at an alarm occurrence.
(→page 9)

IMPORTANT

- When “Polling(30s)” is selected for “Alarm status update mode” (→page 27), the Alarm occurrence indication button will be refreshed in 30-second intervals. For this reason, it may take a maximum of 30 seconds until the alarm occurrence indication button is displayed on the “Live” page at an alarm occurrence.

Transmit an image onto a server automatically

An alarm image can be transmitted at an alarm occurrence to the server designated in advance. The settings required to transmit an alarm image to a server can be configured in the “Alarm image” section on the [Alarm] tab of the “Alarm” page (→page 47) and the [FTP] tab of the “Server” page (→page 62). However, when “D1” is selected for “Picture (Camera) mode”, images cannot be transmitted.

Notify of alarm occurrences by E-mail

Alarm E-mail (alarm occurrence notification) can be sent at an alarm occurrence to the E-mail addresses registered in advance. Up to 4 addresses can be registered as recipients of the alarm E-mail. The settings for alarm E-mail can be configured in the “E-mail notification” section on the [Notification] tab of the [Alarm] page (→page 52) and the [E-mail] tab of the “Server” page (→page 61).

Notify of alarm occurrences to the designated IP addresses (Panasonic alarm protocol notification)

This function is available only when a Panasonic device, such as the network disk recorder, is connected to the system. When “On” is selected for “Panasonic alarm protocol notification”, the connected Panasonic device will be notified that the unit is in the alarm state. The settings for Panasonic alarm protocol can be configured in the Panasonic alarm protocol section of the [Notification] tab of the [Alarm] page. (→page 53)

4 Transmit images onto an FTP server

Images can be transmitted to an FTP server. By configuring the following settings, transmission of images captured at an alarm occurrence or captured at a designated interval to an FTP server will become available.

IMPORTANT

- When using this function, set the user name and the password to access the FTP server to restrict users who can log into the FTP server.
- When "D1" is selected for "Picture (Camera) mode", images cannot be transmitted to the FTP server.

4.1 Transmit an alarm image at an alarm occurrence (Alarm image transmission)

An alarm image can be transmitted at an alarm occurrence to the FTP server. To transmit alarm images to an FTP server, it is necessary to configure the settings in advance.

The settings for the FTP server can be configured on the [FTP] tab of the "Server" page. (→page 62)

The alarm image transmission function can be turned on/off in the "Alarm image" section of the [Alarm] tab of the "Alarm" page. (→page 47)

Note

- Depending on the line speed or the traffic, the number of the transmitted images may not reach the set number of images to be transmitted.

4.2 Transmit images at a designated interval or period (FTP periodic image transmission)

Images can be transmitted at a designated interval or period. To transmit images at a designated interval or period, it is necessary to configure the settings in advance.

The settings for the FTP server can be configured on the [FTP] tab of the "Server" page. (→page 62)

It is possible to determine whether or not to use the FTP periodic image transmission function and to configure the settings relating to alarm images and the schedule on the "FTP img. trans." tab of the "Network" page. (→page 99)

Note

- Depending on the line speed or the traffic, images may not be transmitted at the designated interval.
- When "On" is selected for both the alarm image transmission function and the FTP periodic image transmission function, the alarm image transmission function will be given priority over the FTP periodic image transmission function. Therefore, images may not be transmitted at the interval designated on the "FTP periodic image transmission" setting.

5 About the network security

5.1 Equipped security functions

The following security functions are featured in this unit.

- ① Access restrictions by the host authentication and the user authentication
It is possible to restrict users from accessing the unit by setting the host authentication and/or the user authentication to "On". (→page 56, page 57)
- ② Access restrictions by changing the HTTP port
It is possible to prevent illegal access such as port scanning, etc. by changing the HTTP port number. (→page 69)
- ③ Access encryption by the HTTPS function
It is possible to enhance the network security by encrypting the access to units using the HTTPS function. (→page 74)

IMPORTANT

- Design and enhance security countermeasures to prevent leakage of information such as image data, authentication information (user name and password), alarm E-mail information, FTP server information, DDNS server information, etc. Perform the countermeasure such as access restriction (using the user authentication) or access encryption (using the HTTPS function).
- After the unit is accessed by the administrator, make sure to close all the browsers for added security.
- Change the administrator password periodically for added security.

Note

- When user authentication (authentication error) has failed to pass 8 times within 30 seconds using the same IP address (PC), access to the unit will be denied for a while.

6 Display the setup menu from a PC

The settings of the unit can be configured on the setup menu.

IMPORTANT

- The setup menu is only operable by users whose access level is “1. Administrator”. Refer to page 56 for how to configure the access level.

6.1 How to display the setup menu

1. Display the “Live” page. (→page 7)
2. Click the [Setup] button on the “Live” page.
→ The window with the user name and password entry fields will be displayed.

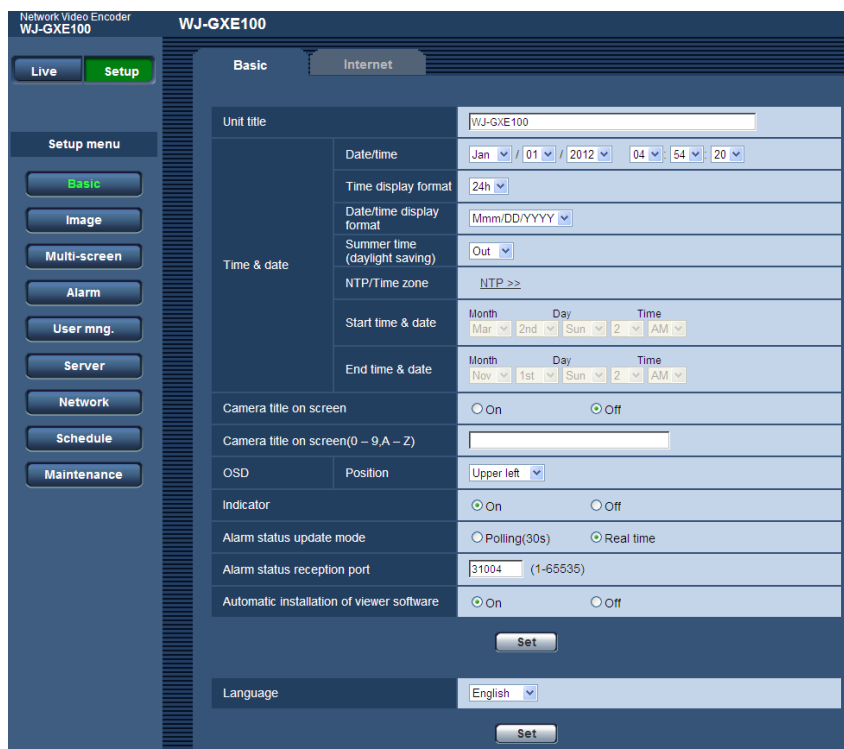


3. Click the [OK] button after entering the user name and the password.
The default user name and password are as follows.
User name: admin
Password: 12345

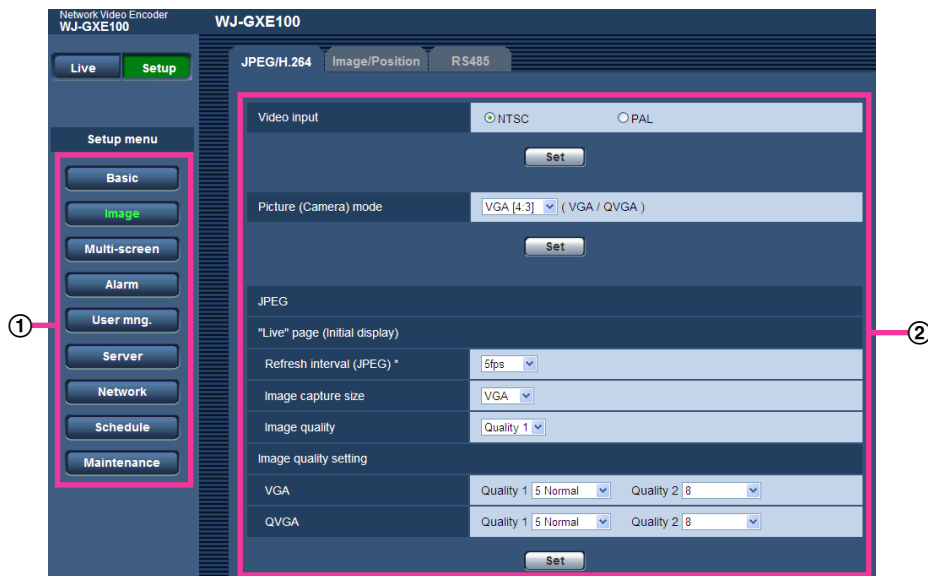
6 Display the setup menu from a PC



→ The setup menu will be displayed. Refer to page 25 for further information about this menu.



6.2 How to operate the setup menu



- ① Menu buttons
- ② Setup page

1. Click the desired button in the frame on the left of the window to display the respective setup menu. When there are tabs at the top of the "Setup" page displayed in the frame on the right of the window, click the desired tab to display and configure the setting items relating to the name of the tab.
2. Complete each setting item displayed in the frame on the right of the window.
3. After completing each setting item, click the [Set] button to apply them.

IMPORTANT

- When there are two or more [Set] and [Execute] buttons on the page, click the respective button to the edited setting item.

6 Display the setup menu from a PC

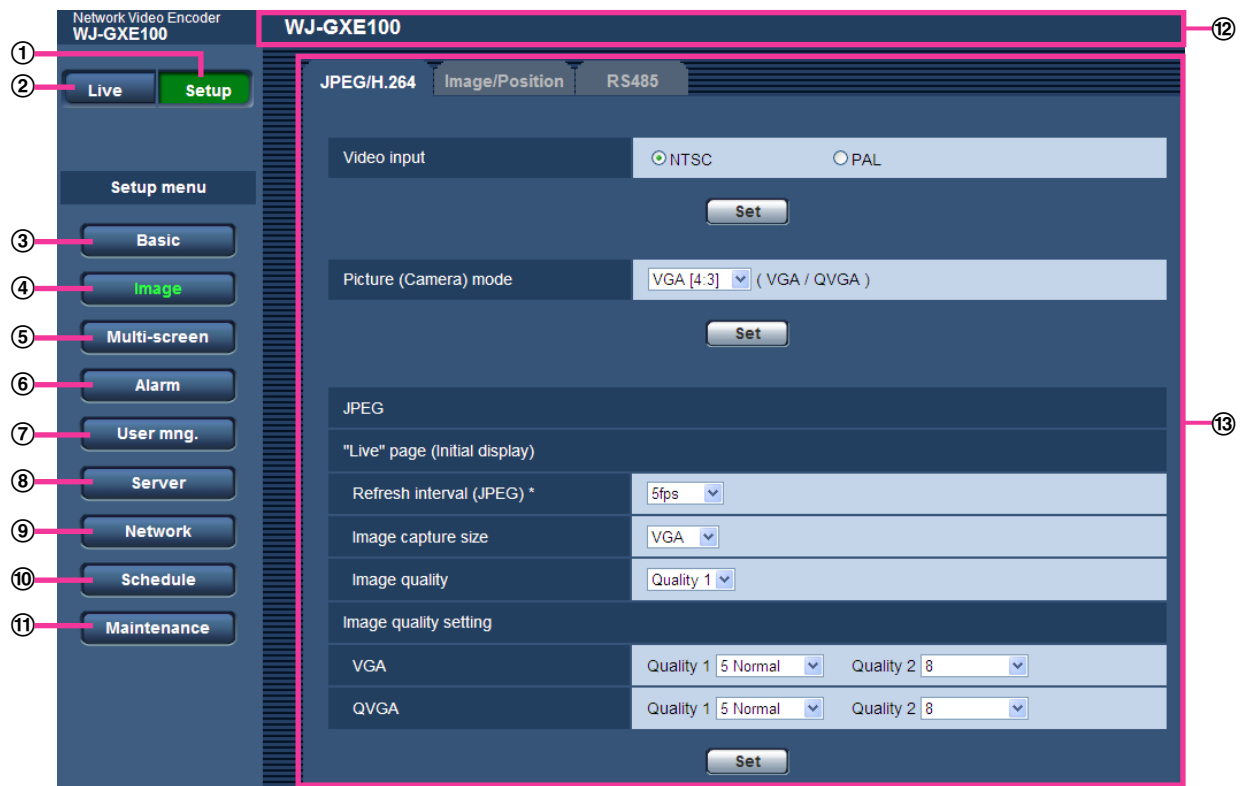
<Example>

The screenshot displays a configuration interface with the following elements and callouts:

- ①** Points to the "Video input" section, which includes radio buttons for "NTSC" (selected) and "PAL".
- ②** Points to the "Set" button located directly below the "Video input" section.
- ③** Points to the "Picture (Camera) mode" section, which includes a dropdown menu currently set to "VGA [4:3]" and the text "(VGA / QVGA)".
- ④** Points to the "Set" button located directly below the "Picture (Camera) mode" section.
- ⑤** Points to the "JPEG" section, which contains several sub-sections: "Live" page (Initial display), "Refresh interval (JPEG) *" (set to "5fps"), "Image capture size" (set to "VGA"), "Image quality" (set to "Quality 1"), and "Image quality setting" (containing "VGA" and "QVGA" rows, each with "Quality 1" and "Quality 2" dropdowns).
- ⑥** Points to the "Set" button located at the bottom of the "JPEG" section.

When completing the setting items in field ①, click the [Set] button (②) below field (①).
The edited settings in field ① will not be applied unless the [Set] button (②) below field (①) is clicked.
In the same manner as above, click the [Set] button (④ and ⑥) below field ③ and ⑤ when completing the setting items in field ③ and ⑤.

6.3 About the setup menu window



- ① **[Setup] button**
Displays the “Setup” page.
- ② **[Live] button**
Displays the “Live” page.
- ③ **[Basic] button**
Displays the “Basic” page. The basic settings such as time and date and the unit title, and the settings required to connect the unit to the Internet can be configured on the “Basic” page. (→page 27)
- ④ **[Image] button**
Displays the “Image” page. The settings relating to image quality, image capture size, etc. of JPEG/H.264 camera images can be configured on the “Image” page. (→page 32)
- ⑤ **[Multi-screen] button**
Displays the “Multi-screen” page. The cameras from which images are to be displayed on a multi-screen can be registered on the “Multi-screen” page. (→page 44)
- ⑥ **[Alarm] button**
Displays the “Alarm” page. The settings relating to alarm occurrences such as settings for the alarm action at an alarm occurrence, the alarm occurrence notification, and the VMD area settings can be configured on the “Alarm” page. (→page 46)
- ⑦ **[User mng.] button**
Displays the “User mng.” page. The settings relating to the authentication such as users and PCs restrictions for accessing the unit can be configured on the “User mng.” page. (→page 56)
- ⑧ **[Server] button**
Displays the “Server” page. The settings relating to the E-mail server, the FTP server and the NTP server to which the unit accesses can be configured on the “Server” page. (→page 61)

⑨ **[Network] button**

Displays the “Network” page. The network settings and the settings relating to DDNS (Dynamic DNS), SNMP (Simple Network Management Protocol) and the FTP (File Transfer Protocol) periodic transmission can be configured on the “Network” page. (→page 66)

⑩ **[Schedule] button**

Displays the “Schedule” page. On the “Schedule” page, it is possible to designate time zones to allow to activate the VMD detection function. (→page 103)

⑪ **[Maintenance] button**

Displays the “Maintenance” page. System log check, firmware upgrade, status check and initialization of the setup menu can be carried out on the “Maintenance” page. (→page 106)

⑫ **Unit title**

The title of the unit whose settings are currently being configured will be displayed.

⑬ **Setup page**

Pages of each setup menu will be displayed. There are tabs for some setup menus.

7 Configure the basic settings of the unit [Basic]

The settings relating to configuring the unit title, time and date, and connecting to the Internet can be configured on the “Basic” page.

The “Basic” page has 2 tabs; the [Basic] tab and the [Internet] tab.

7.1 Configure the basic settings [Basic]

Click the [Basic] tab of the “Basic” page. (→page 21, page 23)

The settings such as the unit title, time and date, etc. can be configured on this page.

The screenshot shows the 'Basic' configuration page. The 'Unit title' is 'WJ-GXE100'. The 'Time & date' section includes settings for date/time (Jan 01 2012 14:44:29), time display format (24h), date/time display format (Mmm/DD/YYYY), summer time (Out), NTP/Time zone (NTP >>), start time & date (Mar 2nd Sun 2 AM), and end time & date (Nov 1st Sun 2 AM). Other settings include 'Camera title on screen' (Off), 'Camera title on screen(0-9,A-Z)' (empty), 'OSD Position' (Upper left), 'Indicator' (On), 'Alarm status update mode' (Real time), 'Alarm status reception port' (31004), and 'Automatic installation of viewer software' (On). The 'Language' is set to 'English'. 'Set' buttons are present below the 'Automatic installation of viewer software' and at the bottom of the page.

[Unit title]

Enter the title of the unit. Click the [Set] button after entering the title of the unit. The entered title will be displayed in the unit title field.

- **Available number of characters:** 0 - 20 characters
- **Unavailable characters:** " &
- **Default:** WJ-GXE100

[Date/time]

Enter the current time and date. When “12h” is selected for “Time display format”, “AM” or “PM” can be selected.

- **Available range:** Jan/01/2010 00:00:00 - Dec/31/2035 23:59:59

IMPORTANT

- Use an NTP server when the more accurate time & date setting is required for the system operation.
(→page 64)

[Time display format]

Select the time display format from “24h”, “12h” and “Off”. Enter the current hour reflecting this setting when entering the current time and date for “Date/time”. To hide time and date, select “Off”.

- **Default:** 24h

[Date/time display format]

Select a date/time display format. When “2010/04/01 13:10:00” is set for “Date/time” after selecting “24h” for “Date/time display format”, time & date will be respectively displayed as follows.

- **DD/MM/YYYY:** 01/04/2010 13:10:00
- **MM/DD/YYYY:** 04/01/2010 13:10:00
- **DD/Mmm/YYYY:** 01/Apr/2010 13:10:00
- **YYYY/MM/DD:** 2010/04/01 13:10:00
- **Mmm/DD/YYYY:** Apr/01/2010 13:10:00
- **Default:**
 - Mmm/DD/YYYY (P model)
 - DD/MM/YYYY (E model)

[Summer time (daylight saving)]

Select “In”, “Out” or “Auto” to determine whether or not to apply daylight saving time. Configure this setting if the summer time (daylight saving time) is applied in the location where the unit is in use.

- **In:** Applies summer time. An asterisk (*) will be displayed on the left side of the displayed time and date.
- **Out:** Does not apply summer time.
- **Auto:** Applies summer time in accordance with the settings for “Start time & date” and “End time & date” (month, week, day of the week, time).
- **Default:** Out

[NTP/Time zone]

When “NTP >>” is clicked, the [NTP] tab of the “Server” page will be displayed. (→page 64)

[Start time & date] [End time & date]

When “Auto” is selected for “Summer time (daylight saving)”, select the time & date for the start time and the date time (month, week, day of the week, time).

[Camera title on screen]

Select “On” or “Off” to determine whether or not to display the camera title on the screen. When “On” is selected, the character string entered for “Camera title on screen (0-9, A-Z)” will be displayed at the position selected for “OSD”.

- **Default:** Off

[Camera title on screen (0-9, A-Z)]

Enter a character string to be displayed on the image.

- **Available number of characters:** 0 - 20 characters
- **Available characters:** 0-9, A-Z and the following marks.
! " # \$ % & ' () * + , - . / : ; = ?

- **Default:** None (blank)

[OSD] - [Position]

Select the position where the time and date and a character string to be displayed on the image of the “Live” page.

- **Upper left:** The above information will be displayed at the upper left corner of the main area on the “Live” page.
- **Lower left:** The above information will be displayed at the lower left corner of the main area on the “Live” page.
- **Upper right:** The above information will be displayed at the upper right corner of the main area on the “Live” page.
- **Lower right:** The above information will be displayed at the lower right corner of the main area on the “Live” page.
- **Default:** Upper left

[Indicator]

Determine whether or not to use the live indicator (POWER).

- **On:** The indicator lights up or blinks in the following manner when the power is turned on.

| | |
|--|----------------------------|
| When the power is turned on | Lights green |
| When connected to a network (not accessed) | Lights orange |
| When connected to a network (accessed) | Blinks orange/Blinks green |

- **Off:** The indicator is turned off at all times.
- **Default:** On

[Alarm status update mode]

Select an interval of the unit status notification from the following.

When the status of the unit changes, the alarm occurrence indication button will be displayed to notify of the unit status.

- **Polling(30s):** Updates the status each 30 seconds and provide notification of the unit status.
- **Real time:** Provide notification of the unit status when the status has changed.
- **Default:** Real time

Note

- Depending on the network environment, notification may not be provided in real time.
- When multiple cameras are using the same “Alarm status reception port”, even if “Real time” is selected for “Alarm status update mode”, status notification is not provided in real time. In this case, change the “Alarm status reception port” settings.

[Alarm status reception port]

When selecting “Real time” for “Alarm status update mode”, designate a port number to which the status change notification is to be sent.

- **Available port number:** 1 - 65535
- **Default:** 31004

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[Automatic installation of viewer software]

Determine whether or not to install the viewer software from this unit.

- **On:** Installs the viewer software from the unit automatically.
- **Off:** The viewer software cannot be installed from the unit.

7 Configure the basic settings of the unit [Basic]

- **Default:** On

IMPORTANT

- It is impossible to display images between the camera and the PC when the viewer software “Network Camera View 4S” is not installed on the PC.
- The number of the viewer software installations can be checked on the [Upgrade] tab of the “Maintenance” page.

[Language]

Select the language to initially display when the unit is accessed from the following.
English/Japanese/Italian/French/German/Spanish/Chinese/Russian

- **Default:** English

The language displayed on the “Live” page can also be changed. (→page 9)

7.2 Configure the Internet settings [Internet]

Click the [Internet] tab of the “Basic” page. (→page 21, page 23)

The settings relating to UPnP (Auto port forwarding), DDNS (Viewnetcam.com), and network settings for the Internet can be configured on this page.

The screenshot shows the 'Internet' tab selected in the 'Basic' configuration menu. It contains two main settings: 'UPnP(Auto port forwarding)' with radio buttons for 'On' and 'Off' (where 'Off' is selected), and 'DDNS' with a dropdown menu set to 'Off'. Below these is a text instruction: 'To allow access to the camera from the Internet, activate the auto port forwarding (IPv4) setting and register on the DDNS service "Viewnetcam.com" (free).' followed by a note: 'Note: The camera may be accessed from a third party if the Internet access is allowed.' and a 'Set' button. At the bottom, there is a section for 'Recommended network setting for internet' with a message 'A setup suitable for internet environment is carried out.' and another 'Set' button.

[UPnP (Auto port forwarding)]

Select “On” or “Off” to determine whether or not to use the port forwarding function of the router.

To use the auto port forwarding function, the router in use must support UPnP and the UPnP must be enabled.

- **Default:** Off

Note

- Due to auto port forwarding, the port number may sometimes be changed. When the number is changed, it is necessary to change the port numbers registered in the PC and recorders, etc.
- The UPnP function is available when the unit is connected to the IPv4 network. IPv6 is not supported.
- To check if auto port forwarding is properly configured, click the [Status] tab on the “Maintenance” page, and check that the “Enable” is displayed for “Status” of “UPnP”. (→page 108)
When “Enable” is not displayed, refer to “Cannot access the unit via the Internet.” in 20 Troubleshooting.
- When the “UPnP (Auto port forwarding)” setting is changed, the “Auto port forwarding” setting under “UPnP” on the [Network] tab of the “Network” page also changes to the same setting.

[DDNS]

Select “Viewnetcam.com” or “Off” to determine whether or not to use “Viewnetcam.com”.

By selecting "Viewnetcam.com" and clicking the [Set] button, the registration window for "Viewnetcam.com" will be displayed in a newly opened window.

Follow the on-screen instructions to register with "Viewnetcam.com".

Refer to page 94 or the "Viewnetcam.com" website (<http://www.viewnetcam.com/>) for further information.

- **Default:** Off

Note

- When the "DDNS" setting is changed, the "DDNS" setting on the [DDNS] tab of the "Network" page also changes to the same setting.

[Recommended network setting for internet]

The recommended settings for connecting to the Internet are performed here.

By clicking the [Set] button, a dialog displaying how the following settings will change is displayed.

Click the [OK] button after checking the settings to change the settings to the displayed values.

- [JPEG/H.264] tab on the "Image" page
 - [H.264(1)]/[H.264(2)]**
 - [Internet mode (over HTTP)]: On
 - [Transmission priority]: Best effort
 - [Max bit rate (per client)*]: Max. 1024 kbps, Min. 128 kbps
 - [H.264(1)]**
 - [Image capture size]: VGA
 - [H.264(2)]**
 - [Image capture size]: QVGA
- [Network] tab on the "Network" page
 - [Common]**
 - [Max RTP packet size]: Limited(1280byte)
 - [HTTP max segment size(MSS)]: Limited(1280byte)

Note

- When "D1" is selected for "Picture (Camera) mode", the resolution remains D1.

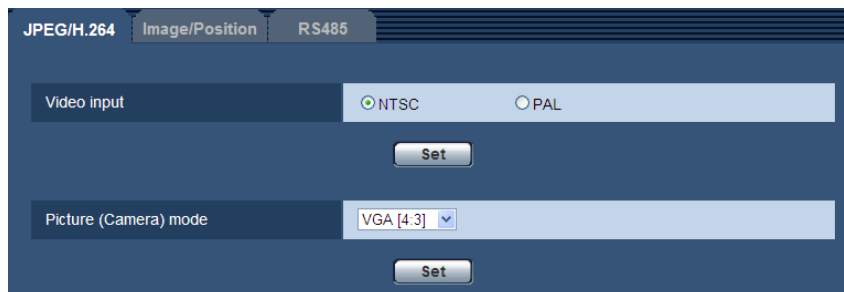
8 Configure the settings relating to images [Image]

The JPEG and H.264 image settings and settings relating to image quality and RS485 can be configured on this page.

The “Image” page has 3 tabs; the [JPEG/H.264] tab, the [Image/Position] tab and the [RS485] tab.

8.1 Configure the settings relating to the Picture (Camera) mode/Video input [JPEG/H.264]

Click the [JPEG/H.264] tab on the “Image” page. (→page 21, page 23)



[Video input]

Select the camera video input from the following.

NTSC/PAL

- **Default:** NTSC (P model), PAL (E model)

Note

- When “NTSC” is selected for “Video input”, the maximum frame rate is 30 fps. When “PAL” is selected, the maximum frame rate is 25 fps.
- When the [Set] button is pressed after changing the “Video input” setting, the settings are reset to the default and the unit is rebooted. Note that the network settings will not be reset.

[Picture (Camera) mode]

Select the picture (camera) mode from the following.

VGA [4:3]/ VGA [16:9]/ D1

- **Default:** VGA [4:3]

Note

- When “Picture (Camera) mode” is changed to “D1” or the mode is changed from “D1” to another mode, the unit will reboot automatically.
- When “D1” is selected for “Picture (Camera) mode”, some of the functions will not be available. (→page 111)
- Refer to our website (<http://panasonic.net/pss/security/support/info.html>) for further information about the support of Panasonic network disk recorders when “D1” is selected for “Picture (Camera) mode”.
- Image/Position adjustment function is activated for the angle of view in “VGA [4:3]” even when “VGA [16:9]” is selected for “Picture (Camera) mode”. Because a part of the connected camera's setup menu will not be displayed in this case, we recommend changing the “Picture (Camera) mode” setting to “VGA [4:3]”.

8.2 Configure the settings relating to JPEG images [JPEG/H.264]

Click the [JPEG/H.264] tab on the “Image” page. (→page 21, page 23)

JPEG

Configure the settings such as “Refresh interval (JPEG)*”, “Image capture size” and “Image quality” on this section. Refer to page 35 for further information about the settings relating to H.264 images.

“Live” page (Initial display)

Configure the settings relating to the JPEG images displayed on the “Live” page.

[Refresh interval (JPEG)*]

Select an interval to refresh the displayed JPEG image from the following.

NTSC: 0.1fps/ 0.2fps/ 0.33fps/ 0.5fps/ 1fps/ 2fps/ 3fps/ 5fps/ 6fps */ 10fps */ 15fps */ 30fps *

PAL: 0.08fps/ 0.17fps/ 0.28fps/ 0.42fps/ 1fps/ 2.1fps/ 3.1fps/ 4.2fps/ 5fps */ 8.3fps */ 12.5fps */ 25fps *

- **Default:**
 - 5fps (NTSC)
 - 4.2fps (PAL)

Note

- When “On” is selected for “H.264 transmission”, the refresh interval may be longer than the set value when any value with an asterisk (*) on the right is selected.
- Depending on factors such as the network environment, the resolution, the image quality, or the number of computers concurrently accessing the unit, the transmission interval may be longer than the set value.
- If images are not delivered in the specified transmission interval, you can make the images be delivered closer to the specified interval by lowering the resolution or image quality.

[Image capture size]

Select the image capture size to display the JPEG image on the “Live” page for the first time.

| | |
|----------------------------------|-----------------|
| Picture (Camera) mode VGA [4:3] | QVGA/VGA |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 |
| Picture (Camera) mode D1 | D1 |

- **Default:** VGA

[Image quality]

Select the image quality of JPEG images displayed initially on the “Live” page.

- **Default:** Quality1

[Image quality setting]

Select two types of image quality of JPEG images for each image capture size.

0 Super fine/ 1 Fine/ 2/ 3/ 4/ 5 Normal/ 6/ 7/ 8/ 9 Low

- **Default:**
 - Quality1: 5 Normal
 - Quality2: 8

The setting for “Quality1” is activated for FTP periodic image transmission.

8.3 Configure the settings relating to H.264 images [JPEG/H.264]

Click the [JPEG/H.264] tab on the “Image” page. (→page 21, page 23)

Configure the settings relating to H.264 image such as “Max bit rate (per client)”, “Image capture size”, “Image quality”, etc. in this section. Refer to page 33 for the settings relating to JPEG images.

| H.264(1) | |
|--|---|
| H.264 transmission | <input checked="" type="radio"/> On <input type="radio"/> Off |
| Internet mode (over HTTP) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Image capture size | VGA |
| Transmission priority | Frame rate |
| Frame rate* | 30fps |
| Max bit rate (per client) * | Max 1536kbps - Min 128kbps |
| Image quality | Normal |
| Refresh interval | 1s |
| Transmission type | Unicast port (AUTO) |
| Unicast port | 32004 (1024-50000) |
| Multicast address | 239.192.0.20 |
| Multicast port | 37004 (1024-50000) |
| Multicast TTL/HOPLimit | 16 (1-254) |
| Set | |
| H.264(2) | |
| H.264 transmission | <input checked="" type="radio"/> On <input type="radio"/> Off |
| Internet mode (over HTTP) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Image capture size | VGA |
| Transmission priority | Frame rate |
| Frame rate* | 30fps |
| Max bit rate (per client) * | Max 1536kbps - Min 128kbps |
| Image quality | Normal |
| Refresh interval | 1s |
| Transmission type | Unicast port (AUTO) |
| Unicast port | 32014 (1024-50000) |
| Multicast address | 239.192.0.21 |
| Multicast port | 37004 (1024-50000) |
| Multicast TTL/HOPLimit | 16 (1-254) |
| Set | |
| Smoother live video display on the browser (buffering) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Set | |

H.264(1)/H.264(2)

[H.264 transmission]

Select "On" or "Off" to determine whether or not to transmit H.264 images.

- **On:** Transmits H.264 images.
- **Off:** Does not transmit H.264 images.
- **Default:** On

Note

- When "On" is selected for "H.264 transmission" in "H.264(1)" or "H.264(2)", displaying of H.264 images or JPEG images on the "Live" page will become available.
- When "On" is selected for "H.264 transmission" in "H.264(1)" and "H.264(2)", H.264 images are viewable using other devices with each setting.
- When "On" is selected for "H.264 transmission" in "H.264(1)" or "H.264(2)", the transmission interval of JPEG images may sometimes become longer.

[Internet mode (over HTTP)]

Select "On" when transmitting H.264 images via the Internet. It is possible to transmit H.264 images without changing the broadband router settings configured for JPEG image transmission.

- **On:** H.264 images will be transmitted using the HTTP port. Refer to page 69 for further information about the HTTP port number settings.
- **Off:** H.264 images will be transmitted using the UDP port.
- **Default:** Off

Note

- When "On" is selected, only "Unicast port (AUTO)" will be available for "Transmission type".
- When "On" is selected, it may take time to start displaying H.264 images.
- When "On" is selected, H.264 images may not be displayed depending on the number of the concurrent access user, etc.
- When "On" is selected, only IPv4 access is available.

[Image capture size]

Select the image capture size from the following.

| | |
|----------------------------------|-----------------|
| Picture (Camera) mode VGA [4:3] | QVGA/VGA |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 |
| Picture (Camera) mode D1 | D1 |

- **Default:** VGA

[Transmission priority]

Select a transmission priority for H.264 images from the following.

- **Constant bit rate:** H.264 images will be transmitted with the bit rate selected for "Max bit rate (per client) *".
- **Frame rate:** H.264 images will be transmitted with the frame rate selected for "Frame rate*".
- **Best effort:** In accordance with the network bandwidth, H.264 images will be transmitted with the bit rate varying between the maximum and minimum bit rates that are set for "Max bit rate (per client)*".
- **Default:** Frame rate

Note

- When "Frame rate" is selected for "Transmission priority", number of users who can access the unit may be limited more (may become less than 10).

[Frame rate*]

Select a frame rate for H.264 images from the following.

NTSC: 1fps/ 3fps/ 5fps */7.5fps */ 10fps */ 15fps */ 20fps */ 30fps *

PAL: 1fps/ 3.1fps/ 4.2fps */ 6.25fps */ 8.3fps */ 12.5fps */ 20fps */ 25fps *

- **Default:**
 - 30fps * (NTSC)
 - 25fps * (PAL)

Note

- When “Frame rate” is selected for “Transmission priority”, this setting is available.
- “Frame rate*” is restricted by “Max bit rate (per client)*”. For this reason, the frame rate may be lower than the specified value when any value marked with an asterisk (*) is selected.

[Max bit rate (per client)*]

Select an H.264 bit rate per a client from the following. When “Best effort” is selected for “Transmission priority”, set the maximum and minimum bit rates.

64kbps/ 128kbps*/ 256kbps*/ 384kbps*/ 512kbps*/ 768kbps*/ 1024kbps*/ 1536kbps*/ 2048kbps*/ 3072kbps*/ 4096kbps*/ Unlimited*

- **Default:** 1536kbps*

“Unlimited*” is available only when “Frame rate” is selected for “Transmission priority”.

Note

- When “Unlimited*” is selected, the number of users who can access H.264 images will be limited to “1”. (Only a single user can access H.264 images.)
- The H.264 bit rate is restricted by “Bandwidth control(bit rate)” on the [Network] tab on the “Network” page (→page 66). For this reason, the bit rate may be lower than the value when any value with an asterisk (*) on the right is selected.
- It is impossible to select “Unlimited*” for both “H.264(1)” and “H.264(2)”.

[Image quality]

Select the image quality of H.264 images from the following.

Low(Motion priority)/ Normal/ Fine(Image quality priority)

- **Default:** Normal

Note

- When “Constant bit rate” or “Best effort” is selected for “Transmission priority”, this setting is available.

[Refresh interval]

Select an interval (I-frame interval; 0.2 - 5 seconds) to refresh the displayed H.264 images.

If using under a network environment with frequent error occurrences, shorten the refresh interval for H.264 to diminish image distortions. However, the refresh interval may be longer than the set value.

0.2s/ 0.25s/ 0.33s/ 0.5s/ 1s/ 2s/ 3s/ 4s/ 5s

- **Default:** 1s

[Transmission type]

Select the transmission type of H.264 images from the following.

- **Unicast port (AUTO):** Up to 14 users can access a single unit concurrently. “Unicast port” will automatically be selected when transmitting images from the unit. When it is unnecessary to fix the port number for H.264 image transmission such as when using in a particular LAN environment, it is recommended to select “Unicast port (AUTO)”.
- **Unicast port (MANUAL):** Up to 14 users can access a single unit concurrently. It is necessary to select “Unicast port” manually to transmit images from the unit.

It is possible to fix the port number of the router used for H.264 image transmission via the Internet by setting "Unicast port (MANUAL)" (→page 66). Refer to the operating instructions of the router in use.

- **Multicast:** Unlimited number of users can access a single unit concurrently. Complete the entry field of "Multicast address", "Multicast port" and "Multicast TTL/HOPLimit" when transmitting H.264 images with multicast. Refer to page 7 for further information about the maximum concurrent access number.
- **Default:** Unicast port (AUTO)

[Unicast port]^{*1}

Enter the unicast port number (used to transmit images from the unit).

- **Available port number:** 1024 - 50000 (Only even numbers are available.)
- **Default:**
 - H.264(1): 32004
 - H.264(2): 32014

[Multicast address]^{*2}

Enter the multicast IP address. Images will be transmitted to the designated IP address.

- **Available IPv4 address:** 224.0.0.0 - 239.255.255.255
- **Available IPv6 address:** Multicast address starting with "FF"
- **Default:**
 - H.264(1): 239.192.0.20
 - H.264(2): 239.192.0.21

Note

- Enter a multicast IP address after checking available multicast address.

[Multicast port]^{*2}

Enter the multicast port number (used to transmit images from the unit).

- **Available port number:** 1024 - 50000 (Only even numbers are available.)
- **Default:** 37004

Note

- The following port numbers are unavailable since they are already in use.
10669, 10670

[Multicast TTL/HOPLimit]^{*2}

Enter a value for "Multicast TTL/HOPLimit".

- **Available value:** 1-254
- **Default:** 16

IMPORTANT

- When transmitting an H.264 image via a network, the transmitted image sometimes may not be displayed depending on the settings of a proxy server or a firewall. In this case, refer to the network administrator.
- When two or more network interface cards are installed on the PC in use, the network interface card(s) not used for receiving images should be invalidated when displaying images using the multicast port.

[Smoother live video display on the browser (buffering)]

Perform settings to display unit images on the viewer software.

- **On:** Images are temporarily stored on the computer and are displayed smoother.
- **Off:** Images are displayed in real-time and are not stored on the computer.
- **Default:** Off

IMPORTANT

- If it appears that there is a delay in the images being displayed, select “Off”.

^{*1} It is necessary to designate the unicast port number when “Unicast port (MANUAL)” is selected for “Transmission type”.

^{*2} It is necessary to designate the multicast IP address when “Multicast” is selected for “Transmission type”.

8.4 Configure the settings relating to image and positions [Image/Position]

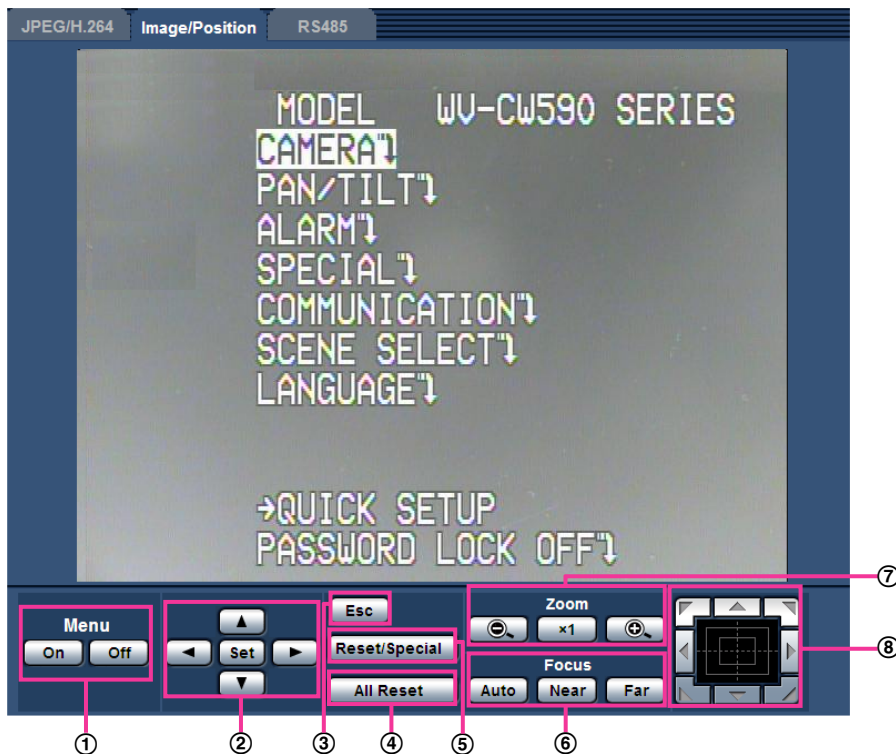
Click the [Image/Position] tab on the “Image” page. (→page 21, page 23)

The image quality and position settings can be configured on this page, by displaying the setup menu on the image using the camera connected to the unit and RS485 communication.

Note

- It is necessary to connect the RS485 cable of the camera to the unit and to set RS485 on the [RS485] tab on the “Image” page. (→page 41)
- Refer to the manuals provided with the camera for the camera setup menu.
- Image/Position adjustment function is activated for the angle of view in “VGA [4:3]” even when “VGA [16:9]” is selected for “Picture (Camera) mode”. Because a part of the connected camera's setup menu will not be displayed in this case, we recommend changing the “Picture (Camera) mode” setting to “VGA [4:3]”. (→page 32)

Example: when the connected camera is WV-CW590



Display the camera's setup menu on the image, and use each button to perform operations as necessary. The displayed setup menu differs depending on the connected camera.

① [Menu] buttons

- **[On] button:** Click this button to display the setup menu of camera.
- **[Off] button:** Click this button to close the setup menu of camera.

② Arrow buttons/[Set] button

- **▲/▼ buttons:** Click these buttons to move the cursor.
- **◀/▶ buttons:** Click these buttons to select the parameters.
- **[Set] button:** Click this button to move the submenu.

③ **[Esc] button**

Click this button to return to the previous page.

④ **[All Reset] button**

Display the camera's setup menu, and then click the [All Reset] button after moving the cursor onto "CAMERA RESET" on the SPECIAL SETUP menu to reset to the default setting. Refer to the operating instructions of each camera for further information about the settings to be reset.

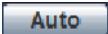
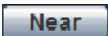

⑤ **[Reset/Special] button**

Display the setup menu of camera, move the cursor onto "SPECIAL", and click this button to move to the SPECIAL SETUP menu.




Move the cursor onto "REFRESH" on the SPECIAL SETUP menu, and click this button to refresh the camera position.

Item names and operations may differ depending on the cameras. Refer to the operating instructions of the camera for further information.

⑥ **[Focus] buttons**

- : Click this button to adjust the focus automatically.
- : Click this button to adjust the focus to the "Near" side.
- : Click this button to adjust the focus to the "Far" side.

⑦ **[Zoom] buttons**

- : Click this button to adjust the zoom ratio to the "Wide" side.
- : Click this button to set the zoom ratio to x1.0.
- : Click this button to adjust the zoom ratio to the "Tele" side.

⑧ **Control pad/buttons**

- Left-click on the control pad or buttons to adjust the horizontal/vertical position of the camera (panning/tilting).
Panning/tilting speed will be faster if a clicked point gets farther from the center point of the control pad. It is also possible to pan/tilt the camera by dragging the mouse.
Zoom and focus can be adjusted by right-clicking. When an upper/lower area of the control pad is right-clicked, the displayed image will be zoomed in/out on. When a left/right area is right-clicked, the focus will be adjusted to the Near/Far side.
Zoom can also be adjusted using the mouse wheel.

8.5 Configure the settings relating to RS485 [RS485]

Click the [RS485] tab on the "Image" page. (→page 21, page 23)

The RS485 settings can be configured on this page to control the camera connected to the unit.

Note

- When cameras with different RS485 protocols (for example, cameras manufactured by Panasonic and Pelco, Inc.) are in the same RS485 communication line, the cameras will not work correctly.
- Select "4-line" or "2-line" according to the RS485 communication method specifications of the connected cameras.
- Refer to our website (<http://panasonic.net/pss/security/support/info.html>) for further information about the control command (command table) of RS485.

8 Configure the settings relating to images [Image]

- The data sent from a PC to the unit through port 52000 of the UDP can be sent to the camera through RS485 to control the camera.

| RS485 | |
|----------------------|--|
| RS485 transmission | <input checked="" type="radio"/> On <input type="radio"/> Off |
| Communication method | <input checked="" type="radio"/> 4-line <input type="radio"/> 2-line |
| Baud rate | 19200bps |
| Data bit | 8bit |
| Parity check | None |
| Protocol | Panasonic |
| Unit address | 01 |

Set

[RS485 transmission]

Select "On" or "Off" to determine whether or not to control the camera using RS485.

- **Default:** On

[Communication method]

Select the communication method of the RS485 cable from 4-line and 2-line.

- **Default:** 4-line

[Baud rate]

Select the line speed for RS485 transmission from the following.

2400bps/4800bps/9600bps/19200bps/38400bps

- **Default:** 19200bps

[Data bit]

Select the data bit from 7bit or 8bit.

- **Default:** 8bit

[Parity check]

Select from the following to determine whether or not to perform the parity check.

None/Odd/Even

- **Default:** None

[Protocol]

Select the RS485 control command for the camera from the following.

Panasonic/Pelco-D/Pelco-P/Custom

- **Default:** Panasonic

Note

- When using RS485 control commands other than Panasonic, Pelco-D, and Pelco-P, select "Custom" for "Protocol" and upload the command table to the unit via an FTP server. The unit must be rebooted after the upload is completed.
- If Pan/Tilt/Zoom functions cannot be operated for Panasonic cameras, you must select "Custom" for "Protocol" and upload the command table to the unit. For further information, refer to our website (<http://panasonic.net/pss/security/support/info.html>).
- Refer to our website (<http://panasonic.net/pss/security/support/info.html>) for further information about how to upload command tables and cases when RS485 cannot control cameras.

- Command table settings are initialized when the unit is initialized. In this case, upload the command tables again as necessary.

[Unit address]

Specify the unit address of the camera connected to the unit.

- **Default:** 01

9 Configure the multi-screen settings [Multi-screen]

Network cameras and units used to display images on a multi-screen can be registered on the “Multi-screen” page. (→page 21, page 23)

Multi-screen

| Group A | IP address | Camera title |
|---------|------------|--------------|
| Cam. 1 | selfcamera | WJ-GXE100 |
| Cam. 2 | | |
| Cam. 3 | | |
| Cam. 4 | | |

Example of entry: http://192.168.0.10:8080

Set

| Group B | IP address | Camera title |
|---------|------------|--------------|
| Cam. 5 | | |
| Cam. 6 | | |
| Cam. 7 | | |
| Cam. 8 | | |

Example of entry: http://192.168.0.10:8080

Set

| Group C | IP address | Camera title |
|---------|------------|--------------|
| Cam. 9 | | |
| Cam. 10 | | |
| Cam. 11 | | |
| Cam. 12 | | |

Example of entry: http://192.168.0.10:8080

Set

| Group D | IP address | Camera title |
|---------|------------|--------------|
| Cam. 13 | | |
| Cam. 14 | | |
| Cam. 15 | | |
| Cam. 16 | | |

Example of entry: http://192.168.0.10:8080

Set

[IP address]

Enter the IP address or the host name of the unit or network camera to be used for the multi-screen. 4 cameras can be registered as a group and up to 4 groups (16 cameras) can be registered.

When the HTTP port number for the unit or network camera of which images are to be displayed had been changed, enter as follows:

Example of entry:

- **Example when entering an IPv4 address:** http://192.168.0.10:8080
- **Example when entering an IPv6 address:** http://[2001:db8:0:0:0:0:1]:8080

To access the units using the HTTPS protocol, enter as follows:

Example of entry: https://192.168.0.10/

- **Available number of characters:** 1 - 128 characters
- **Default:** (Cam. 1) selfcamera, (Cam. 2 - 16) not registered

IMPORTANT

- This unit is specified when “selfcamera” is displayed for the IP address or host name.
- “Network Camera Recorder with Viewer Software Lite” which supports live monitoring and recording images from multiple cameras is available. For further information, refer to our website (<http://panasonic.net/pss/security/support/info.html>).
- When accessing the unit using the HTTPS protocol, install the security certificate of the camera to display images on the monitor. (→page 81)

Note

- When using the host name, it is necessary to configure the DNS settings of the PC to be used for the multi-screen display. Refer to the network administrator for information on the DNS setting of PCs.

[Camera title]

Enter the title of the camera. The entered camera title will be displayed on a multi-screen.

- **Available number of characters:** 0 - 20 characters
- **Unavailable characters:** " &
- **Default:** (Cam. 1) WJ-GXE100, (Cam. 2 - 16) None (blank)

Note

- When selecting a 16 split-screen, some characters of the camera title to be displayed may not be displayed.
- When displaying images on multi-screen from the unit or network cameras that have the aspect ratio configured to a setting other than “4:3”, the image will be displayed altered to the aspect ratio of “4:3”.

10 Configure the alarm settings [Alarm]

The settings relating to alarm occurrences such as settings for the alarm action at an alarm occurrence, the VMD area settings, and the alarm occurrence notification can be configured on this page.

The “Alarm” page has 3 tabs; the [Alarm] tab, the [VMD area] tab and the [Notification] tab.

10.1 Configure the settings relating to the alarm action [Alarm]

Click the [Alarm] tab on the “Alarm” page. (→page 21, page 23)

The settings relating to the alarm can be configured in this section. Refer to page 47 for further information about the settings relating to the alarm images.

| Alarm | |
|-------------------------|---|
| VMD alarm | VMD >> |
| Command alarm | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Originating port number | <input type="text" value="8181"/> (1-65535) |
| Video loss alarm | <input type="radio"/> On <input checked="" type="radio"/> Off |

Alarm

[VMD alarm]

When clicking “VMD >>”, the [VMD area] tab of the “Alarm” page will be displayed.

[Command alarm]

Select “On” or “Off” to determine whether or not to receive the command alarm.

The command alarm is the function that provides notification of a Panasonic protocol alarm from the other cameras. When “On” is selected, alarm actions will be performed between multiple cameras.

- **Default:** Off

[Originating port number]

Select a port number to be used to receive the command alarm.

- **Available range:** 1-65535
- **Default:** 8181

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 554, 995, 10669, 10670, 52000, 59000-61000

[Video loss alarm]

Select “On” or “Off” to determine whether or not to activate the alarm when a video loss occurs.

- **Default:** Off

10.2 Configure the settings relating to the alarm image [Alarm]

Click the [Alarm] tab on the “Alarm” page. (→page 21, page 23)

The settings relating to the alarm image to be transmitted to an FTP server can be configured in this section. The alarm image will be transmitted to an FTP server. To transmit alarm images to an FTP server, it is necessary to configure the settings in advance. (→page 62)

IMPORTANT

- When “D1” is selected for “Picture (Camera) mode”, alarm images cannot be transmitted.
- Depending on the network line speed or the network traffic, images may not be transmitted at the exact designated interval or period.

| Alarm image | | | |
|---|---|------------------------------|----------------------------|
| Alarm image FTP transmission | <input type="radio"/> On <input checked="" type="radio"/> Off | | |
| Directory name | <input type="text"/> | | |
| File name | <input type="text"/> | | |
| Post alarm | Transmission interval 1fps | Number of Images 100 pics | Recording duration 100s |
| Image capture size | VGA | | |
| Image compression rate upon alarm detection | <input type="radio"/> On <input checked="" type="radio"/> Off | | |
| Image quality upon alarm detection | 5 Normal | | |
| <input type="button" value="Set"/> | | | |

Alarm image

[FTP >>]

When “FTP >>” is clicked, the [FTP] tab of the “Server” page will be displayed. (→page 62)

[Alarm image FTP transmission]

Select “On” or “Off” to determine whether or not to transmit the alarm image to the FTP server.

- **Default:** Off

[Directory name]

Enter the directory name where the alarm images are to be saved.

For example, enter “/ALARM” to designate the directory “ALARM” under the root directory of the FTP server.

- **Available number of characters:** 1 - 256 characters
- **Unavailable characters:** " & ;
- **Default:** None (blank)

[File name]

Enter the file name used for the alarm image to be transmitted to an FTP server. The file name will be as follows.

File name: [“Entered file name” + “Time and date (year/ month/ day/ hour/ minute/ second)”] + “Serial number”

- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & * / : ; < > ? \ |
- **Default:** None (blank)

[Post alarm]

- **Transmission interval**

Select the transmission interval for the alarm image transmission to the FTP server from the following.

NTSC: 0.1fps/ 0.2fps/ 0.33fps/ 0.5fps/ 1fps

PAL: 0.08fps/ 0.17fps/ 0.28fps/ 0.42fps/ 1fps

- **Default:** 1fps

- **Number of images**

Select the number of images to be transmitted from the following.

1pic/ 2pics/ 3pics/ 4pics/ 5pics/ 6pics/ 7pics/ 8pics/ 9pics/ 10pics/ 20pics/ 30pics/ 50pics/ 100pics/ 200pics/ 300pics/ 500pics/ 1000pics/ 2000pics/ 3000pics

- **Default:** 100pics

- **Recording duration**

Approximate time to be taken to save the set "Number of images" with the set "Transmission interval" will be displayed.

[Image capture size]

Select the capture size of images to be transmitted to the FTP server or of an image to be attached to the alarm E-mail.

| | |
|----------------------------------|-----------------|
| Picture (Camera) mode VGA [4:3] | QVGA/VGA |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 |

- **Default:** VGA

[Image compression rate upon alarm detection]

Select "On" or "Off" to determine whether or not to change the image quality of "Quality1" (→page 33) upon alarm detection.

- **On:** Images will be transmitted with the image quality selected for "Image quality upon alarm detection".
- **Off:** Does not change the image quality upon alarm detection.
- **Default:** Off

[Image quality upon alarm detection]

Image quality can be changed upon an alarm occurrence. Select the image quality from the following.

0 Super fine/ 1 Fine/ 2/ 3/ 4/ 5 Normal/ 6/ 7/ 8/ 9 Low

- **Default:** 5 Normal

10.3 Configure the VMD settings [VMD area]

Click the [VMD area] tab on the "Alarm" page. (→page 21, page 23)

The VMD areas can be set on this page.

Up to 4 areas can be set. When motion is detected in the set area, it will be regarded as an alarm.

IMPORTANT

- The alarm occurrence indication button (→page 9) will be displayed when motion is detected by the VMD function.
- The alarm occurrence indication button will be displayed when receiving a command alarm or video loss alarm.
- Depending on the network environment, notification may be delayed even when "Real time" is selected for "Alarm status update mode" on the [Basic] tab of the "Basic" page (→page 27).

- The VMD function is not the dedicated function to prevent thefts, fires, etc. We are not responsible for any accidents or damages occurring in case.

| Area | 1(White) | 2(Blue) | 3(Green) | 4(Red) |
|-----------------------|--|---|---|---|
| Status | <input type="radio"/> On <input checked="" type="radio"/> Off | <input type="radio"/> On <input checked="" type="radio"/> Off | <input type="radio"/> On <input checked="" type="radio"/> Off | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Detection area | 1 | 1 | 1 | 1 |
| Detection sensitivity | Low High 8 | Low High 8 | Low High 8 | Low High 8 |
| Delete | <input type="button" value="Delete"/> | <input type="button" value="Delete"/> | <input type="button" value="Delete"/> | <input type="button" value="Delete"/> |
| Area No. notification | Panasonic alarm protocol notification >> | | | |

* When notifying alarm area numbers by the Panasonic alarm protocol, set "Additional alarm area data(VMD)" to "On".

VMD information addition

Information addition ☐ On ☒ Off

[Area]

When selecting a VMD area in the screen, it will be numbered as area 1. (Subsequent areas will be numbered in the order of selection.)

[All areas] button

When the [All areas] button is clicked, the whole area will become the VMD area, and "1(White)" will be automatically applied to "Area".

[Status]

Select "On" or "Off" to determine whether or not to perform video motion detection.

- On:** Performs video motion detection.
- Off:** Does not perform video motion detection.
- Default:** Off

[Detection area]

Adjust the size of the VMD area using the slider. The smaller the selected value is, the higher the sensitivity of VMD area becomes. The current value (1-10) will be displayed on the right of the slider.

- **Default:** 1

[Detection sensitivity]

Adjust the sensitivity of motion detection in the VMD area using the slider. The settings can be configured for each area individually. The larger the value is set, the higher the sensitivity level becomes.

The current value (1 (low) - 15 (high)) will be displayed below the slider.

- **Default:** 8

[Delete] button

Click the [Delete] button corresponding to the area to be deleted. The outline of the selected area will be deleted.

[Area No. notification]

When "Panasonic alarm protocol notification >>" is clicked, the [Notification] tab of the "Alarm" page will be displayed. (→page 53)

VMD information addition

[Information addition]

Select "On" or "Off" to determine whether or not to add VMD information to superimposed image data.

The VMD information can be searched by some of Panasonic network disk recorders. Refer to the operating instructions of the connected devices for further information about the functions and settings.

- **Default:** Off

Note

- When the camera is performing pan, tilt, zoom, or focus operations, adjusting the brightness, or operating in auto mode, VMD information is added.

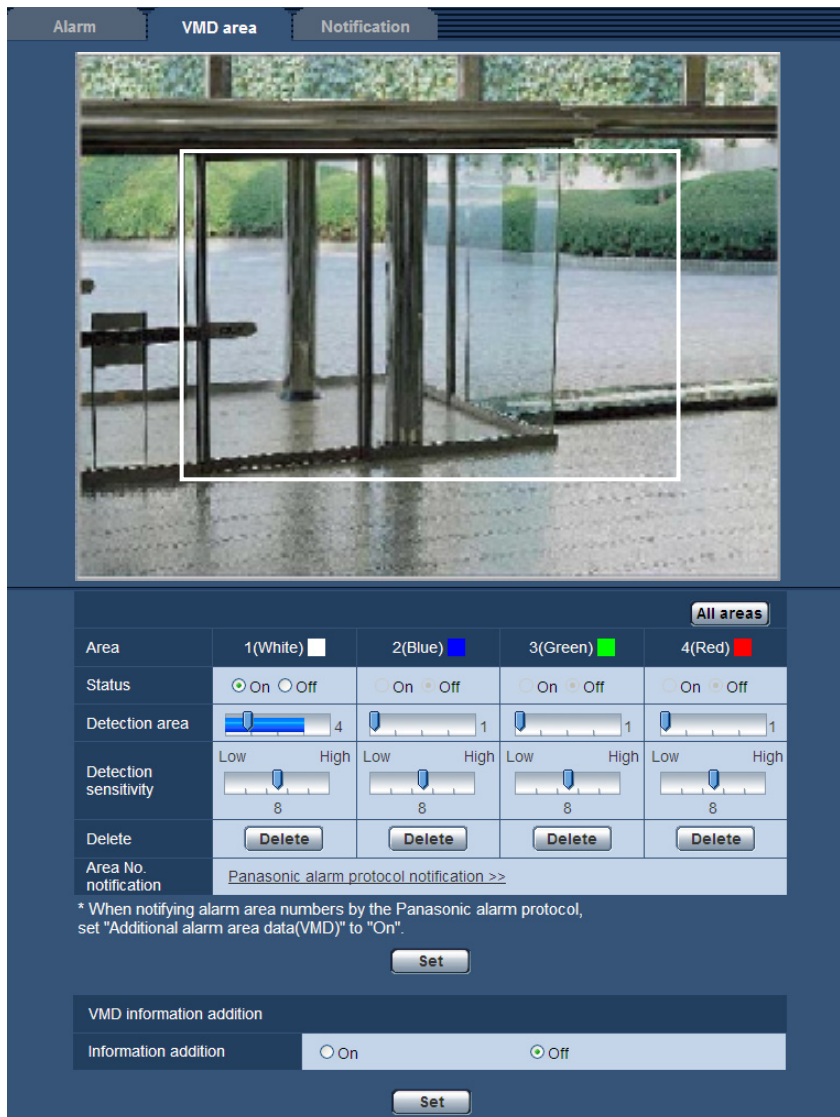
10.3.1 Set the VMD areas [VMD area]

Set the areas to activate the VMD function.

IMPORTANT

- When the settings are being configured on the setup menu, sometimes the VMD function may not work correctly.

- Set the video motion detection area by dragging the mouse on the screen.
 → The designated area will become the VMD area "1(White)" and the outline will be displayed. When 2 - 4 VMD areas are set, each area will be numbered in order. The areas will be identified by the respective outline colors. The "Status" of the outline to be set for the area will become "On".



- Adjust "Detection area" and "Detection sensitivity" using the slider. "Detection area" can be adjusted by moving the slider between the left end position and the center position. "Detection sensitivity" can be adjusted by moving the slider between the left end position and the right end position. Refer to page 48 for further information about the "Detection sensitivity" and "Detection area". The currently displayed area and its detection sensitivity will be displayed in the "Detection area" section. When the status bar exceeds the setting position of slider, the alarm action will be performed. Change areas and the settings of "Detection area" and "Detection sensitivity" as necessary.

Note

- When "Detection area" cannot be adjusted properly by moving the slider, adjust "Detection sensitivity" while checking the motion detection status.

3. Click the [Set] button after completing the settings.

IMPORTANT

- The setting will not be applied unless the [Set] button is clicked.
4. To invalidate the VMD area, click the [Set] button after selecting “Off” for “Status” of the VMD area to be invalidated.
 - The outline of the invalidated VMD area will turn to a dotted line. When the VMD area is invalidated, no alarm will occur even when a motion can be recognized in the area.
 5. To delete the VMD area, click the [Delete] button corresponding to the area to be deleted.
 - The outline of the respective VMD area will disappear.
 6. Click the [Set] button.
 - The edited settings will be applied.

10.4 Configuration of the settings relating to the E-mail notification [Notification]

Click the [Notification] tab on the “Alarm” page. (→page 21, page 23)

The settings relating to the alarm E-mail can be configured. It is necessary to configure the settings of the E-mail server to perform the E-mail notification. (→page 61)

| Destination of notification | Alarm | Destination E-mail address |
|-----------------------------|--------------------------|--|
| Address 1 | <input type="checkbox"/> | <input type="text"/> <input type="button" value="Delete"/> |
| Address 2 | <input type="checkbox"/> | <input type="text"/> <input type="button" value="Delete"/> |
| Address 3 | <input type="checkbox"/> | <input type="text"/> <input type="button" value="Delete"/> |
| Address 4 | <input type="checkbox"/> | <input type="text"/> <input type="button" value="Delete"/> |

E-mail notification

[E-mail server >>]

When “E-mail server >>” is clicked, the [E-mail] tab of the “Server” page will be displayed. (→page 61)

[E-mail notification]

Select “On” or “Off” to determine whether or not to provide notification by E-mail according to the settings for the “Alarm” and “Diag.” checkboxes of “Destination of notification” below.

- When an alarm is detected (“Alarm”)
- **Default:** Off

Destination of notification

[Address 1] - [Address 4]

Enter the destination E-mail address. Up to 4 destination E-mail addresses can be registered.

- **[Alarm] checkbox:** When the checkbox is selected, the E-mail notification will be sent when an alarm occurs or when a video loss is recovered.
- **[Destination E-mail address]:** Enter the destination E-mail address.
 - **Available number of characters:** 3 - 128 characters
 - **Available characters:** Alphanumeric characters, the at sign (@), the period (.), the underscore (_), and the hyphen (-).
 - **Default:** None (blank)

To delete the registered address, click the [Delete] button respective to the desired address.

[E-mail subject]

Enter the E-mail subject.

- **Available number of characters:** 0 - 50 characters
- **Default:** None (blank)

[E-mail body]

Enter the E-mail body.

- **Available number of characters:** 0 - 200 characters
- **Default:** None (blank)

10.5 Configure the settings relating to Panasonic alarm protocol [Notification]

Click the [Notification] tab on the “Alarm” page. (→page 21, page 23)

10 Configure the alarm settings [Alarm]

The settings relating to Panasonic alarm protocol can be configured in this section.

| Panasonic alarm protocol notification | |
|---------------------------------------|---|
| Panasonic alarm protocol | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Additional alarm area data (VMD) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Destination port | 1818 (1-65535) |
| Retry times | 2 |

Set

| Destination of notification | Alarm | Destination server address |
|-----------------------------|--------------------------|-----------------------------|
| Address 1 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 2 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 3 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 4 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 5 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 6 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 7 | <input type="checkbox"/> | <input type="text"/> Delete |
| Address 8 | <input type="checkbox"/> | <input type="text"/> Delete |

Set

Panasonic alarm protocol notification

[Panasonic alarm protocol]

Select "On" or "Off" to determine whether or not to provide notification by Panasonic alarm protocol according to the settings for the "Alarm" and "Diag." checkboxes of "Destination of notification" below.

- When an alarm is detected ("Alarm")
- When a video loss is recovered ("Alarm")
- **Default:** Off

Note

- When "On" is selected, notification of the alarm occurrence will be provided to the registered destination server addresses in order (to IP address 1 first, to IP address 8 last).

[Additional alarm area data(VMD)]

Determine whether or not to send notifications for the alarm area number of VMD alarm with the Panasonic alarm protocol by selecting On/Off.

- **Default:** Off

[Destination port]

Select a destination port for the Panasonic alarm protocol from the following.

- **Available range:** 1 - 65535
- **Default:** 1818

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[Retry times]

Select a retry time for the Panasonic alarm protocol.

- **Available range:** 0-30
- **Default:** 2

Destination of notification

[Address 1] - [Address 8]

Enter the destination IP address or host name of the Panasonic alarm protocol from the following. Host name is unavailable for the IP address. Up to 8 destination server addresses can be registered.

- **[Alarm] checkbox:** When the checkbox is selected, the Panasonic alarm notification will be sent when an alarm occurs or when a video loss is recovered.
- **[Destination server address]:** Enter the destination server address or host name.
 - **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
 - **Default:** None (blank)

To delete the registered destination server address, click the [Delete] button respective to the desired destination server address.

IMPORTANT

- When entering the host name of the “Destination server address”, the DNS settings on the [Network] tab of the “Network” page must be configured. (→page 66)
- Confirm that the destination IP addresses are registered correctly. When a registered destination does not exist, notification may be delayed.

11 Configure the settings relating to the authentication [User mng.]

The settings relating to the authentication such as users and PCs restrictions for accessing the unit with a PC or cellular phone/mobile terminal can be configured on the “User mng.” page.

The “User mng.” page has 3 tabs; the [User auth.] tab, the [Host auth.] tab and the [System] tab.

11.1 Configure the settings relating to the user authentication [User auth.]

Click the [User auth.] tab on the “User mng.” page. (→page 21, page 23)

The settings relating to the authentication of users who can access this unit from the PC or a cellular phone/mobile terminal can be configured on this page. Up to 18 users can be registered.

Note

- When user authentication has failed to pass (authentication error) 8 times within 30 seconds using the same IP address (PC), access to the unit will be denied for a while.

[User auth.]

Select “On” or “Off” to determine whether or not to authenticate the users.

- Default:** Off

[Authentication]

Set the user authentication method.

Digest or Basic: Uses Digest or Basic authentication.

Digest: Uses Digest authentication.

Basic: Uses Basic authentication.

- Default:** Digest or Basic

Note

- When the [Authentication] setting has been changed, close the web browser, and then access the unit again.

- For other devices such as network disk recorders, unless otherwise stated, Digest authentication is not supported. (As of December, 2012)

[User name]

Enter a user name.

- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & ; \

[Password] [Retype password]

Enter a password.

- **Available number of characters:** 4 - 32 characters
- **Unavailable characters:** " &

Note

- When the user name already in use is entered and the [Set] button is clicked, the respective user information will be overwritten.

[Access level]

Select the access level of the user from the following.

- **1. Administrator:** Allowed all available operations of the unit.
- **2. Camera control:** Allowed to display images from the camera and to control the unit. The unit setting configuration is unavailable.
- **3. Live only:** Only displaying live images is available. The unit setting configuration and unit control are unavailable.
- **Default:** 3. Live only

[User check]

From the pull-down menu of "User check", the registered user can be selected and the selected user's information can be checked.

The registered user will be displayed with the access level.

(Example: admin [1])

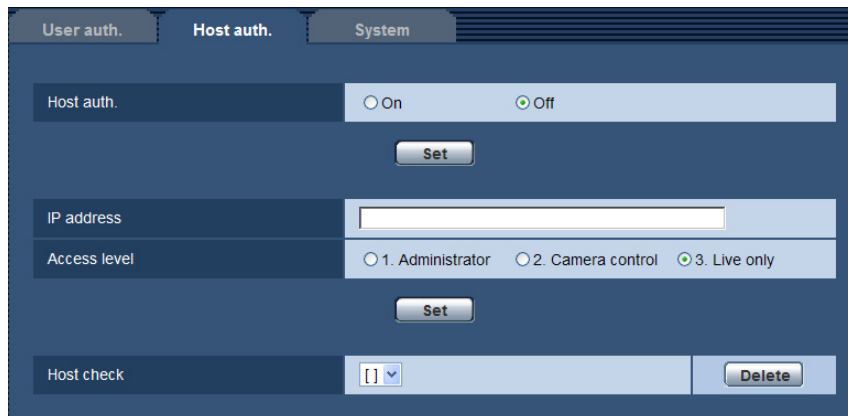
To delete the registered user, click the [Delete] button after selecting the user to be deleted.

11.2 Configure the settings relating to the host authentication [Host auth.]

Click the [Host auth.] tab on the "User mng." page. (→page 21, page 23)

11 Configure the settings relating to the authentication [User mng.]

The restriction settings of PCs (IP address) from accessing the unit can be configured on this page.



[Host auth.]

Select “On” or “Off” to determine whether or not to authenticate the host.

- **Default:** Off

[IP address]

Enter the IP address of the PC to be allowed to access the camera. Host name cannot be entered for the IP address.

Note

- When “IP address/subnet mask” is entered, it is possible to restrict PCs in each subnet. For example, when “192.168.0.1/24” is entered and “2. Camera control” is selected for the access level, the PCs whose IP address is between “192.168.0.1” - “192.168.0.254” can access the camera with the access level “2. Camera control”.
- When the IP address already in use is entered and the [Set] button is clicked, the respective host information will be overwritten.

[Access level]

Select the access level of the host from the following.

1. Administrator/ 2. Camera control/ 3. Live only

Refer to page 56 for further information about the access level.

- **Default:** 3. Live only

[Host check]

From the pull-down menu of “Host check”, the registered host can be selected and the selected host’s IP address can be checked.

The registered IP address will be displayed with the access level.

(Example: 192.168.0.21 [1])

To delete the registered host, click the [Delete] button after selecting the IP address to be deleted.

11.3 Configure the settings relating to the priority stream [System]

Click the [System] tab on the “User mng.” page. (→page 21, page 23)

The description below is the configuration of the priority stream that can transmit images without deteriorating the image quality and refresh interval even when multiple users access concurrently.

| User auth. | Host auth. | System |
|------------------------------------|---|--------|
| Priority stream | | |
| Activation | <input type="radio"/> On <input checked="" type="radio"/> Off | |
| Destination IP address(1) | <input type="text"/> | |
| Destination IP address(2) | <input type="text"/> | |
| Stream type | JPEG ▼ | |
| Refresh interval* | 1fps ▼ | |
| Image capture size | VGA ▼ | |
| <input type="button" value="Set"/> | | |

Priority stream

[Activation]

Select “On” or “Off” to determine whether or not to use the priority stream.

- **Default:** Off

Note

- When “On” is selected for “Activation” of “Priority stream”, number of users who can access the camera may be limited.

[Destination IP address(1)]

Enter the first destination IP address.

- **Default:** None (blank)

[Destination IP address(2)]

Enter the second destination IP address.

- **Default:** None (blank)

[Stream type]

Select either “JPEG”, “H.264(1)” or “H.264(2)”.

- **JPEG:** JPEG images will be transmitted.
- **H.264(1):** H.264(1) images will be transmitted.
- **H.264(2):** H.264(2) images will be transmitted.
- **Default:** JPEG

Note

- When “Best effort” is selected for “Transmission priority” of “H.264”, bit rate will vary between the maximum and minimum rates while images are being transmitted.

[Refresh interval*]

Select the refresh interval from the following.

This setting is validated only when “JPEG” is selected for “Stream type”.

NTSC: 0.1fps/ 0.2fps/ 0.33fps/ 0.5fps/ 1fps/ 2fps/ 3fps/ 5fps/ 6fps * / 10fps * / 15fps * / 30fps *

PAL: 0.08fps/ 0.17fps/ 0.28fps/ 0.42fps/ 1fps/ 2.1fps/ 3.1fps/ 4.2fps/ 5fps * / 8.3fps * / 12.5fps * / 25fps *

- **Default:** 1fps

11 Configure the settings relating to the authentication [User mng.]

Note

- When “On” is selected for “H.264 transmission”, the transmission interval may be longer than the set value when any value with an asterisk (*) on the right is selected.

[Image capture size]

Select the image capture size from the following.

This setting is validated only when “JPEG” is selected for “Stream type”.

| | |
|----------------------------------|-----------------|
| Picture (Camera) mode VGA [4:3] | QVGA/VGA |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 |
| Picture (Camera) mode D1 | D1 |

- **Default:** VGA

12 Configure the settings of the servers [Server]

The settings relating to the E-mail server, the FTP server and the NTP server can be configured on this page. The “Server” page has 3 tabs; the [E-mail] tab, the [FTP] tab and the [NTP] tab.

12.1 Configure the settings relating to the E-mail server [E-mail]

Click the [E-mail] tab on the “Server” page. (→page 21, page 23)

The settings relating to the E-mail server used to send the alarm E-mail can be configured on this page.

IMPORTANT

- When a terminal that receives E-mails is not compatible with UTF-8 encode, it is impossible to receive alarm E-mails correctly.

The screenshot shows a web-based configuration interface for email settings. At the top, there are three tabs: 'E-mail', 'FTP', and 'NTP'. The 'E-mail' tab is selected. Below the tabs, there are several input fields and a 'Set' button at the bottom. The fields include: 'SMTP server address' (a text box), 'SMTP port' (a text box with '25' and a range '(1-65535)' next to it), 'POP server address' (a text box), 'Authentication' (a section with a 'Type' row containing three radio buttons: 'None' (selected), 'POP before SMTP', and 'SMTP'), 'User name' (a text box), 'Password' (a text box), and 'Sender's E-mail address' (a text box). The 'Set' button is located at the bottom center of the form.

[SMTP server address]

Enter the IP address or the host name of the SMTP server used to send E-mails.

- Available number of characters:** 1 - 128 characters
- Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- Default:** None (blank)

[SMTP port]

Enter the port number to which E-mails are sent.

- Available port number:** 1-65535
- Default:** 25

The following port numbers are unavailable since they are already in use.

20, 21, 23, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[POP server address]

When “POP before SMTP” is selected for “Type”, enter the IP address or the host name of the POP server.

- Available number of characters:** 1 - 128 characters
- Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).

- **Default:** None (blank)

IMPORTANT

- When entering the host name for “SMTP server address” or “POP server address”, it is necessary to configure the DNS settings on the [Network] tab of the “Network” page. (→page 66)

[Authentication]

- **Type**
Select the authentication method to send E-mails from the following.
 - **None:** It is not necessary to clear any authentication to send E-mails.
 - **POP before SMTP:** It is necessary to first clear the POP server authentication to use the SMTP server to send E-mails.
 - **SMTP:** It is necessary to clear the SMTP server authentication to send E-mails.
 - **Default:** None

Note

- When you don't know the authentication method to send E-mails, refer to the network administrator.
- **User name**
Enter the user name to access the server.
 - **Available number of characters:** 0 - 32 characters
 - **Unavailable characters:** " & ; \
 - **Default:** None (blank)
- **Password**
Enter the password to access the server.
 - **Available number of characters:** 0 - 32 characters
 - **Unavailable characters:** " &
 - **Default:** None (blank)

[Sender's E-mail address]

Enter the E-mail address of a sender.

The entered E-mail address will be displayed in the “From” (sender) line of the sent E-mails.

- **Available number of characters:** 3 - 128 characters
- **Available characters:** Alphanumeric characters, the at sign (@), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

12.2 Configure the settings relating to the FTP server [FTP]

Click the [FTP] tab on the “Server” page. (→page 21, page 23)

The settings relating to the FTP server used to transmit the alarm images can be configured on this page.

[FTP server address]

Enter the IP address or the host name of the FTP server.

- **Available number of characters:** 1 - 128 characters
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

IMPORTANT

- When entering the host name for “FTP server address”, it is necessary to configure the DNS settings on the [Network] tab of the “Network” page. (→page 66)

[User name]

Enter the user name (login name) to access the FTP server.

- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & ; \
- **Default:** None (blank)

[Password]

Enter the password to access the FTP server.

- **Available number of characters:** 0 - 32 characters
- **Unavailable characters:** " &
- **Default:** None (blank)

[Control port]

Enter a control port number to be used for the FTP server.

- **Available port number:** 1-65535
- **Default:** 21

The following port numbers are unavailable since they are already in use.

20, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[FTP mode]

Select “Passive” or “Active” for the FTP mode.

Normally, select “Passive”. When it is impossible to connect after select “Passive”, try to connect after selecting “Active”.

- **Default:** Passive

12.3 Configure the settings relating to the NTP server [NTP]

Click the [NTP] tab on the “Server” page. (→page 21, page 23)

The settings relating to the NTP server such as the NTP server address, port number, etc. can be configured on this page.

IMPORTANT

- Use an NTP server when the more accurate time & date setting is required for the system operation.

[Time adjustment]

Select the time adjustment method from the following. Time adjusted by the selected method will be used as the standard time of the unit.

- **Manual:** Time set on the [Basic] tab on the “Basic” page will be used as the standard time of the unit.
- **Synchronization with NTP server:** Time automatically adjusted by synchronizing with the NTP server will be used as the standard time of the unit.
- **Default:** Manual

[NTP server address setting]

When “Synchronization with NTP server” is selected for “Time adjustment”, select the method of how to obtain the NTP server address from the following.

- **Auto:** Obtains the NTP server address from the DHCP server.
- **Manual:** The NTP server address will be entered manually on “NTP server address”.
- **Default:** Manual

IMPORTANT

- When obtaining the NTP server address from the DHCP server, it is necessary to select “DHCP”, “Auto(AutoIP)”, or “Auto(Advanced)” for “Network Settings” on the [Network] tab of the “Network” page. (→page 66)

[NTP server address]

When “Manual” is selected for “NTP server address setting”, enter the IP address or the host name of the NTP server.

- **Available number of characters:** 1 - 128 characters
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

IMPORTANT

- When entering the host name for “NTP server address”, it is necessary to configure the DNS settings on the [Network] tab of the “Network” page. (→page 66)

[NTP port]

Enter a port number of the NTP server.

- **Available port number:** 1 - 65535
- **Default:** 123

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 161, 162, 443, 995, 10669, 10670

[Time adjustment interval]

Select an interval (1 - 24 hours: in 1 hour intervals) of synchronization with the NTP server.

- **Default:** 1h

[Time zone]

Select a time zone corresponding to the location where the unit is in use.

- **Default:** (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

13 Configuring the network settings [Network]

The network settings and the settings relating to DDNS (Dynamic DNS), SNMP (Simple Network management Protocol), and FTP image transfer can be configured on the “Network” page.

The “Network” page has 4 tabs; the [Network] tab, the [DDNS] tab, the [SNMP] tab and the [FTP img. trans.] tab.

13.1 Configure the network settings [Network]

Click the [Network] tab on the “Network” page. (→page 21, page 23)

The following information is required to configure the network settings. Contact the network administrator or your Internet service provider.

- IP address
- Subnet mask
- Default gateway (when using the gateway server/router)
- HTTP port
- Primary DNS address, Secondary DNS address (when using DNS)

Network DDNS SNMP FTP img. trans.

IPv4 network

Network Settings: Auto(Advanced) ▼

IP address(IPv4): 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

DNS: ☒ Auto ☐ Manual

Primary server address: 0 . 0 . 0 . 0

Secondary server address: 0 . 0 . 0 . 0

IPv6 network

Manual: ☐ On ☒ Off

IP address(IPv6):

Default gateway:

DHCPv6: ☐ On ☒ Off

Primary DNS server address:

Secondary DNS server address:

Common

HTTP port: 80 (1-65535)

Line speed: Auto ▼

Max RTP packet size: ☒ Unlimited(1500byte) ☐ Limited(1280byte)

HTTP max segment size(MSS): Unlimited(1460byte) ▼

Set

UPnP

Auto port forwarding: ☐ On ☒ Off

Short cut to unit: ☐ On ☒ Off

Set

HTTPS

CRT key generate: Execute

Self-signed Certificate: Generate Execute

Information: Not generated Confirm Delete

Generate Certificate Signing Request: Execute

CA Certificate: CA Certificate install

Invalid Confirm Delete

Connection: HTTP ▼

HTTPS port: 443 (1-65535)

Set

FTP access to unit: ☐ Allow ☒ Forbid

Set

Bandwidth control(bit rate): Unlimited ▼

Set

Easy IP Setup accommodate period: ☒ 20min ☐ Unlimited

Set

IPv4 network

[Network Settings]

Select the method of how to configure the IP address from the following.

- **Static:** The IP address is configured by entering manually on “IP address(IPv4)”.
- **DHCP:** The IP address is configured using the DHCP function.
- **Auto(AutoIP):** The IP address is configured using the DHCP function. When the DHCP server is not found, the IP address is automatically configured.
- **Auto(Advanced):** Using the DHCP function, network address information is referred to, and an unused IP address is configured to the unit as a static IP address. The configured IP address is automatically determined within the subnet mask range by the unit. When the DHCP server is not found, the IP address is set to 192.168.0.10.

- **Default:** Auto(Advanced)

Note

- When “Auto(AutoIP)” is selected and the IP address cannot be obtained from the DHCP server, an IP address not used in the same network will be searched within 169.254.1.0 - 169.254.254.255.

[IP address(IPv4)]

When not using the DHCP function, enter the IP address of the unit. Do not enter an IP address already in use (for the PCs and the other network cameras).

- **Default:** 192.168.0.10

Note

- Multiple IP addresses are unavailable even when using the DHCP function. Refer to the network administrator for further information about the settings of the DHCP server.

[Subnet mask]

When not using the DHCP function, enter the subnet mask of the unit.

- **Default:** 255.255.255.0

[Default gateway]

When not using the DHCP function, enter the default gateway of the unit.

- **Default:** 192.168.0.1

Note

- Multiple IP addresses for the default gateway are unavailable even when using the DHCP function. Refer to the network administrator for further information about the settings of the DHCP server.

[DNS]

Determine how to set the address of the DNS server by selecting “Auto” (obtain the address automatically) or “Manual” (enter the address of the DNS server). When “Manual” is selected, it is necessary to configure the settings for the DNS.

When using the DHCP function, it is possible to obtain the DNS address automatically by selecting “Auto”. Refer to the network administrator for further information about the settings.

- **Default:** Auto

[Primary server address], [Secondary server address]

When “Manual” is selected for “DNS”, enter the IP address of the DNS server. Refer to the network administrator about the IP address of the DNS server.

- **Default:** None (blank)

IPv6 network

[Manual]

Select “On” or “Off” to determine whether or not to manually configure the IP address for IPv6 network (IPv6 address).

- **On:** Enter an IPv6 address manually.
- **Off:** Manual entry of an IPv6 address will become unavailable.
- **Default:** Off

[IP address(IPv6)]

When “On” is selected for “Manual”, manual entry of the IPv6 address is required. Do not enter an address already in use.

Note

- When connecting to the manually configured IPv6 address beyond the router, use an IPv6 compatible router and turn on the automatic IPv6 address assignment function. In this case, it is necessary to configure IPv6 address including prefix information provided from the IPv6 compatible router. Refer to the manuals provided with the router for further information.

[Default gateway]

When “On” is selected for “Manual” of IPv6 network, enter the default gateway of IPv6 network of the unit.

- **Default:** None (blank)

[DHCPv6]

Select “On” or “Off” to determine whether or not to use the IPv6 DHCP function.

Configure the DHCP server not to assign the same IP addresses used for the other network cameras and PCs whose IP address is unique. Refer to the network administrator for further information about the settings of the server.

- **Default:** Off

[Primary DNS server address], [Secondary DNS server address]

Enter the IPv6 address of the DNS server. Refer to the network administrator about the IPv6 address of the DNS server.

- **Default:** None (blank)

Common**[HTTP port]**

Assign the port numbers independently.

- **Available port number:** 1 - 65535
- **Default:** 80

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 110, 123, 161, 162, 443, 554, 995, 10669, 10670, 52000, 59000 - 61000

[Line speed]

Select the line speed for data transmission from the following. It is recommended to use with the default “Auto”.

- **Auto:** Line speed will be applied automatically.
- **100M-Full:** 100 Mbps full-duplex
- **100M-Half:** 100 Mbps half-duplex
- **10M-Full:** 10 Mbps full-duplex
- **10M-Half:** 10 Mbps half-duplex
- **Default:** Auto

[Max RTP packet size]

Select “Unlimited(1500byte)” or “Limited(1280byte)” to determine whether or not to restrict the RTP packet size when viewing images from the camera using the RTP protocol. It is recommended to use with the default “Unlimited(1500byte)”.

When the RTP packet size is restricted in the network line in use, select “Limited(1280byte)”. Refer to the network administrator for further information about the maximum packet size in the network line.

- **Default:** Unlimited(1500byte)

[HTTP max segment size(MSS)]

Select “Unlimited(1460byte)”, “Limited(1280byte)”, or “Limited(1024byte)” to determine whether or not to restrict the maximum segment size (MSS) when viewing images from the camera using the HTTP protocol. We recommended that you use this feature with the default setting.

When the MSS is restricted in the network line in use, select “Limited(1024byte)” or “Limited(1280byte)”. Refer to the network administrator for further information about the MSS in the network line.

- **Default:** Unlimited(1460byte)

UPnP

This unit support UPnP (Universal Plug and Play). By using the UPnP function, it becomes possible to configure the following automatically.

- Configuration of the port forwarding function of the router (However, a router supporting UPnP is required.) This configuration is useful when accessing the unit via the Internet, or from a cellular phone/mobile terminal.
- Automatic refreshment of the shortcut to the unit that is created on the [My Network Places] folder ([Network] folder when using Windows Vista or Windows 7) of the PC even when the IP address of the unit changes.

[Auto port forwarding]

Select “On” or “Off” to determine whether or not to use the port forwarding function of the router.

To use the port forwarding function, the router in use must support UPnP and the UPnP must be enabled.

- **Default:** Off

Note

- Due to port forwarding, the port number may sometimes be changed. When the number is changed, it is necessary to change the port numbers registered in the PC and recorders, etc.
- The UPnP function is available when the unit is connected to the IPv4 network. IPv6 is not supported.
- To check if auto port forwarding is properly configured, click the [Status] tab on the “Maintenance” page, and check that the “Enable” is displayed for “Status” of “UPnP”. (→page 108)
When “Enable” is not displayed, refer to “Cannot access the unit via the Internet.” in the “20 Troubleshooting” section. (→page 122)

[Short cut to unit]

Select whether or not to create the shortcut to the unit on the [My Network Places] folder ([Network] folder when using Windows Vista or Windows 7) of the PC. When creating the shortcut, select “On”.

To use the shortcut function to the unit, enable the UPnP function on the PC in advance.

- **Default:** Off

Note

- To display the shortcut to the unit on the [My Network Places] folder ([Network] folder when using Windows Vista or Windows 7) of the PC, it is necessary to add the Windows component. Refer to the following to enable the UPnP function.

For Windows XP

[Start] → [Settings] → [Control Panel] → [Add or Remove Programs] → [Add/Remove Windows Components] → select [Networking Services] → [Details] → check [Internet Gateway Device Discovery and Control Client] and [UPnP User Interface] → [OK] → [Next] → Complete

For Windows Vista

[Start] → [Control Panel] → [Network and Internet] → [Network and Sharing Center] → expand the section of [Network discovery] of [Sharing and Discovery] → select [Turn on network discovery] → click [Apply] → Complete

For Windows 7

[Start] → [Control Panel] → [Network and Internet] → [Network and Sharing Center] → select [Turn on network discovery] of [Network discovery] of [Change advanced sharing settings] → click [Save changes] → Complete

HTTPS

It is possible to enhance the network security by encrypting the access to units using the HTTPS function. Refer to page 74 for how to configure the HTTPS settings.

[CRT key generate]

CRT key (SSL encryption key) used for the HTTPS protocol is generated. To generate the CRT key, click the [Execute] button to display "CRT key generate" dialog box.

[Self-signed Certificate - Generate]

The unit itself generates the security certificate used for the HTTPS protocol. (Self-signed certificate)
To generate the self-signed certificate, click the [Execute] button to display the "Self-signed Certificate - Generate" dialog box.

[Self-signed Certificate - Information]

Displays the information of the self-signed certificate.

When the [Confirm] button is clicked, the registered information of the self-signed certificate will be displayed in the "Self-signed Certificate - Confirm" dialog box.

When the [Delete] button is clicked, the generated self-signed certificate will be deleted.

[CA Certificate - Generate Certificate Signing Request]

When using the security certificate issued by CA (Certificate Authority) as the security certificate used for the HTTPS protocol, the CSR (Certificate Signing Request) will be generated.

To generate the CSR, click the [Execute] button to display the "CA Certificate - Generate Certificate Signing Request" dialog window.

[CA Certificate - CA Certificate install]

Installs the server certificate (security certificate) issued by CA (Certificate Authority) and displays the information of the installed server certificate.

To install the server certificate, click the [Browse...] button to display the [Open] dialog box, and select the file of the server certificate issued by CA, and click the [Execute] button.

If the server certificate is already installed, the file name of the installed server certificate will be displayed.

[CA Certificate - Information]

Displays the information of the server certificate.

When the [Confirm] button is clicked, the registered information of the installed server certificate will be displayed in the "CA Certificate - Confirm" dialog box. If the server certificate is not installed, the content of the generated CSR file will be displayed.

When the [Delete] button is clicked, the installed server certificate will be deleted.

IMPORTANT

- Before deleting the valid server certificate (security certificate), confirm that there is a backup file on the PC or another media. The backup file will be required when installing the server certificate again.

[Connection]

Select the protocol used to connect the unit.

- **HTTP:** Only the HTTP connection is available.
- **HTTPS:** Only the HTTPS connection is available.
- **Default:** HTTP

[HTTPS port]

Designate the HTTPS port number to be used.

- **Available port number:** 1 - 65535
- **Default:** 443

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 554, 995, 10669, 10670, 52000, 59000-61000

Note

- The unit will restart after the connection setting is changed.
- **When using the self-signed certificate:**
If the unit is accessed using the HTTPS protocol for the first time, the warning window will be displayed. In this case, follow the instructions of the wizard to install the self-signed (security) certificate. (→page 81)
- **When using the server certificate:**
In advance, install the root certificate and intermediate certificate on the browser in use. Follow the instructions of CA for how to obtain and install these certificates.
- When the unit is accessed using the HTTPS protocol, the refresh interval and frame rate of images may be lower.
- When the unit is accessed using the HTTPS protocol, it may take time to display images.
- When the unit is accessed using the HTTPS protocol, the images may be distorted.
- The maximum number of concurrent access user varies depending on the maximum image size and transmission format.

[FTP access to unit]

Select "Allow" or "Forbid" to determine whether to allow or forbid the FTP access to unit.

- **Default:** Forbid

[Bandwidth control(bit rate)]

Select the total bit rate for data transmission from the following.

Unlimited/ 64kbps/ 128kbps/ 256kbps/ 384kbps/ 512kbps/ 768kbps/ 1024kbps/ 2048kbps/ 4096kbps/ 8192kbps

- **Default:** Unlimited

Note

- Select "128kbps" or a faster rate to carry out the live transmission of JPEG images and the FTP periodic image transmission simultaneously.
- When "Bandwidth control(bit rate)" is set low, taking a picture using the snap shot button may not function depending on the use environment. In this case, select "QVGA" for "Image capture size" of "JPEG" on the [JPEG/H.264] tab or set "Image quality setting" of "JPEG" lower.

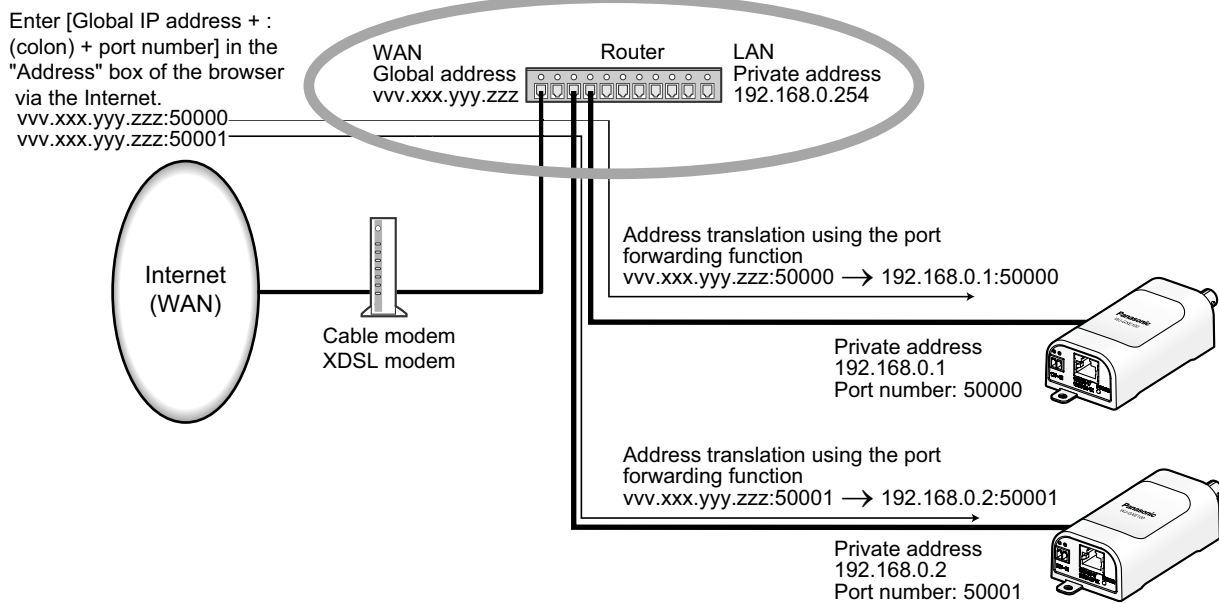
[Easy IP Setup accommodate period]

Select "20min" or "Unlimited" to determine how long the network setting operation using the Panasonic "IP Setting Software" can be allowed.

- **20min:** The network setting operation using the Panasonic "IP Setting Software" are allowed for 20 minutes since the unit starts up.
- **Unlimited:** The network setting operation using the Panasonic "IP Setting Software" are allowed without time limitation.
- **Default:** 20min

Note

- The camera information display using the Panasonic “IP Setting Software” is allowed without time limitation, and unit images can be opened.
- Refer to the network administrator for the addresses of each server.
- The port forwarding function changes a global IP address to a private IP address, and “Static IP masquerade” and “Network Address Translation (NAT)” have this function. This function is to be set in a router.
- To access the unit via the Internet by connecting the unit to a router, it is necessary to assign a respective HTTP port number for each unit and address translation by using the port forwarding function of the router. For further information, refer to the operating instructions of the router in use.

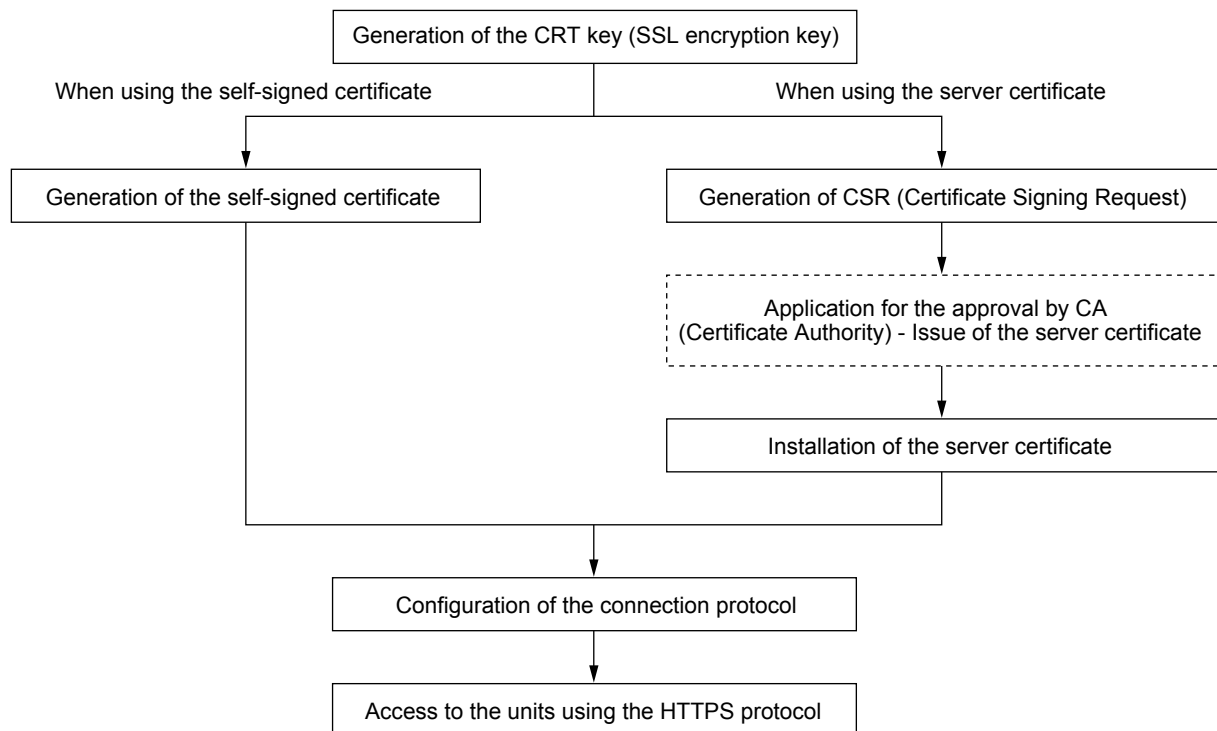


13.2 Configure the HTTPS settings

Click the [Network] tab on the “Network” page. (→page 21, page 23)

The settings relating to the HTTPS protocol that can enhance the network security by encrypting the access to units on this page.

The HTTPS settings will be configured in the following procedure.



The screenshot shows the 'HTTPS' configuration page. It has a table-like structure with sections for 'CRT key generate', 'Self-signed Certificate', 'CA Certificate', 'Connection', and 'HTTPS port'. Numbered callouts point to specific elements: ① points to the 'Execute' button for 'CRT key generate'; ② points to the 'Generate' button for 'Self-signed Certificate'; ③ points to the 'Execute' button for 'Generate Certificate Signing Request'; ④ points to the 'Execute' button for 'CA Certificate install'; ⑤ points to the 'Connection' dropdown menu.

- ① Generation of the CRT key (SSL encryption key) (→page 75)
- ② Generation of the self-signed certificate (→page 76)
- ③ Generation of CSR (Certificate Signing Request) (→page 78)
- ④ Installation of the server certificate (→page 79)
- ⑤ Configuration of the connection protocol (→page 80)

Note

- To use the server certificate, you need to apply for the approval and the issue of server certificate by CA.
- Either of the self-signed certificate or the server certificate is available. If both of them are installed, the server certificate will be used prior to the self-signed certificate.

13.2.1 Generation of the CRT key (SSL encryption key)

IMPORTANT

- When the self-signed certificate or server certificate is valid, it is impossible to generate the CRT key.
 - When the server certification is used, the available key size varies depending on the Caches the available key size in advance.
 - To generate the CRT key, it may take about 1 minute when the key size is 1024 bit and about 2 minutes when the key size is 2048 bit. Do not operate the web browser until the generation of CRT key is complete. While the CRT key is being generated, the refresh interval and line speed may be lower.
1. Click the [Execute] button of “CRT key generate”.
→ The “CRT key generate” dialog box will be displayed.

| Current CRT key | | |
|-----------------|---------------|---------------|
| CRT key | RSA key size | |
| | Last modified | Not generated |

History

CRT key generate

RSA key size ☒ 1024bit ☐ 2048bit Execute

*Generating a CRT key takes around 2 minutes.

Close

2. Select “1024bit” or “2048bit” for the length of the CRT to generate for “CRT key generate” - “RSA key size”.

Note

- To use the server certificate, follow the requests from the CA about the RSA key size.

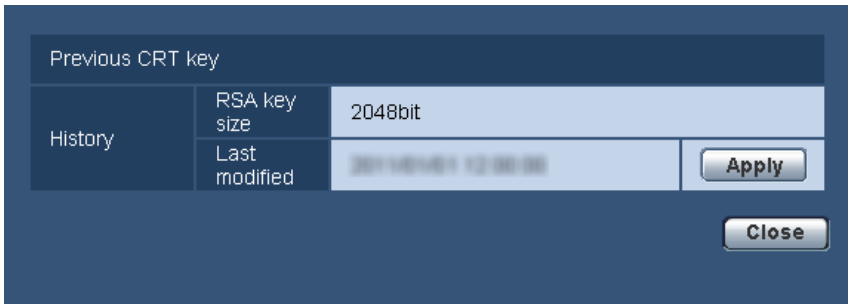
3. Click the [Execute] button.

→ The generation of CRT key will be started. When the generation is finished, the key size and generation time & date of the generated key will be displayed on “Current CRT key”.

Note

- To change (or update) the generated CRT key, perform step 1 to 3. The CRT key, self-signed certificate and server certification are valid in a set. When the CRT key is changed, it is necessary to re-generate the self-signed certificate or re-apply for the server certificate.
- When the CRT key is updated, the log of the previous CRT key is saved. When the [History] button of “Current CRT key” on the “CRT key generate” dialog box is clicked, the “Previous CRT key” dialog box will be displayed, and it is possible to check the key size and generation time & date of the previous

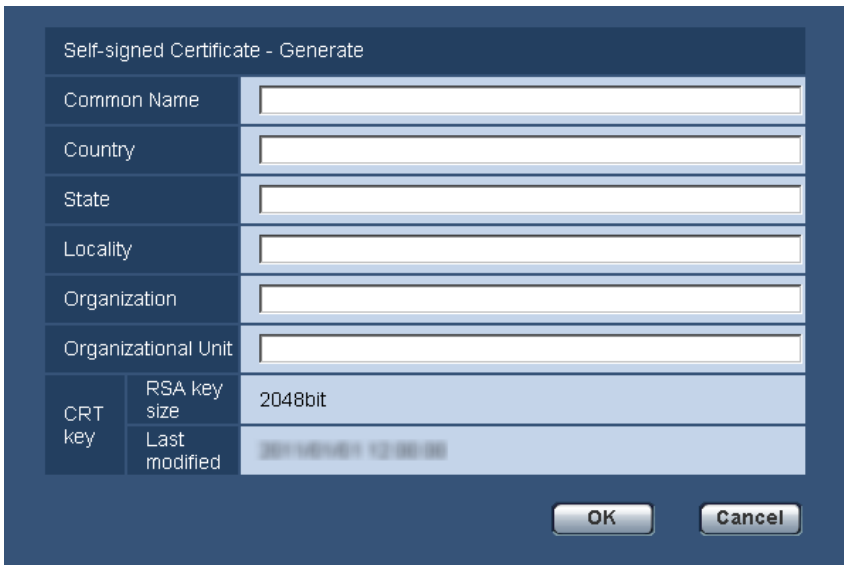
key. When the [Apply] button is clicked on the “Previous CRT key” dialog box, it is possible to replace the current CRT key with the previous one.



13.2.2 Generation of the self-signed certificate (security certificate)

IMPORTANT

- If the CRT key is not generated, it is impossible to generate the self-signed certificate.
1. Click the [Execute] button of “Self-signed Certificate - Generate”.
→ The “Self-signed Certificate - Generate” dialog box will be displayed.



2. Enter the information of the certificate to be generated.

| Item | Description | Available number of characters |
|----------------|--|--------------------------------|
| [Common Name] | Enter the unit address or host name. | 64 characters |
| [Country] | Enter the country name. (Omission is OK.) | 2 characters (Country code) |
| [State] | Enter the state name. (Omission is OK.) | 128 characters |
| [Locality] | Enter the locality name. (Omission is OK.) | 128 characters |
| [Organization] | Enter the organization name. (Omission is OK.) | 64 characters |

| Item | Description | Available number of characters |
|-----------------------|--|--------------------------------|
| [Organizational Unit] | Enter the unit name of the organization. (Omission is OK.) | 64 characters |
| [CRT key] | Displays the key size and generation time & date of the current key. | |

Note

- The available characters for [Common Name], [State], [Locality], [Organization], [Organizational Unit] are 0-9, A-Z, a-z and the following marks.
- . _ , + / ()
- When the unit is connected to the Internet, enter the address name or host name to access via the Internet for "Common Name". In this case, the security alert window will be displayed each time the unit is locally accessed, even if the security certificate is installed.
- When entering the IPv6 address for "Common Name", put the address in brackets [].

Example: [2001:db8::10]

- Click the [OK] button after entering the items.
→ The self-signed certificate will be generated.

Note

- The information of the generated self-signed certificate will be displayed on "Self-signed Certificate" - "Information".

Depending on the status of the self-signed certificate, the following are displayed.

| Indication | Description |
|--|--|
| Not generated | The self-signed certificate are not generated. |
| Invalid (Reason: CA Certificate installed) | The self-signed certificate has already been generated, and the server certificate has been installed. <ul style="list-style-type: none"> In this case, the server certificate is validated. |
| Common name of the self-signed certificate | The self-signed certificate has already been generated and validated. |

- When the [Confirm] button is clicked, the registered information of the self-signed certificate (security certificate) will be displayed in the "Self-signed Certificate - Confirm" dialog box.

Self-signed Certificate - Confirm

| | | |
|---------------------|---------------|---------------------|
| Common Name | NWCAM | |
| Country | | |
| State | | |
| Locality | | |
| Organization | | |
| Organizational Unit | | |
| CRT key | RSA key size | 2048bit |
| | Last modified | 2011-04-01 12:00:00 |

Close

- When the [Delete] button is clicked, the generated self-signed certificate (security certificate) will be deleted.
- When “HTTPS” is selected for “Connection”, it is impossible to delete the self-signed certificate.

13.2.3 Generation of CSR (Certificate Signing Request)

IMPORTANT

- If the CRT key is not generated, it is impossible to generate the CSR.
 - Before generating the CSR file, configure the following settings on [Internet Options] of the web browser in advance. Click [Internet Options...] under [Tools] of the menu bar of Internet Explorer, and then click the [Security] tab.
 - Register the unit for [Trusted Sites].
 - Click the [Custom Level...] button to open the [Security Setting] window, and check the [Enable] radio button of [File Download] under [Downloads].
 - Click the [Custom Level...] button to open the [Security Setting] window, and check the [Enable] radio button of [Automatic prompting for file downloads] under [Downloads].
1. Click the [Execute] button of “CA Certificate - Generate Certificate Signing Request”.
→ The “CA Certificate - Generate Certificate Signing Request” dialog box will be displayed.

2. Enter the information of the certificate to be generated.

| Item | Description | Available number of characters |
|-----------------------|--|--------------------------------|
| [Common Name] | Enter the unit address or host name. | 64 characters |
| [Country] | Enter the country name. | 2 characters (Country code) |
| [State] | Enter the state name. | 128 characters |
| [Locality] | Enter the locality name. | 128 characters |
| [Organization] | Enter the organization name. | 64 characters |
| [Organizational Unit] | Enter the unit name of the organization. | 64 characters |

| Item | Description | Available number of characters |
|-----------|--|--------------------------------|
| [CRT key] | Displays the key size and generation time & date of the current key. | |

Note

- To use the server certificate, follow the requests from the CA about the information to be entered.
 - The available characters for [Common Name], [State], [Locality], [Organization], [Organizational Unit] are 0-9, A-Z, a-z and the following marks.
- . _ , + / ()
3. Click the [OK] button after entering the items.
→ The [Save As] dialog box will be displayed.
 4. Enter a file name for the CSR in the [Save As] dialog box to save on the PC.
→ The saved CSR file will be applied to the CA.

IMPORTANT

- The server certificate will be issued for the set of the generated CSR and CRT key. If the CRT key is re-generated or updated after applying to the CA, the issued server certificate will be invalidated.

Note

- This unit generates the CSR file in the PEM format.

13.2.4 Installation of the server certificate

IMPORTANT

- If the CSR file is not generated, it is impossible to install the server certificate (security certificate). For the installation, the server certificate issued by CA is required.
1. Click the [Browse...] button of "CA Certificate - CA Certificate install".
→ The [Open] dialog box will be displayed.
 2. Select the server certification file and click the [Open] button. Then, click the [Execute] button.
→ The server certification will be installed.

Note

- The host name registered in the installed server certificate will be displayed on "CA Certificate - Information". Depending on the status of the server certificate, the following are displayed.

| Indication | Description |
|---------------------------------------|--|
| Invalid | The server certification is not installed. |
| Common name of the server certificate | The server certificate has already been installed and validated. |
| Expired | The server certification has already expired. |

- When the [Confirm] button is clicked, the registered information of the installed server certificate will be displayed in the “CA Certificate - Confirm” dialog box. (Only “Organizational Unit” will be displayed with an asterisk (*).)

| CA Certificate - Confirm | |
|--------------------------|------------------|
| Common Name | NWCAM |
| Country | JP |
| State | Kagawa |
| Locality | Takamatsu |
| Organization | Panasonic |
| Organizational Unit | Group |
| CRT key | |
| RSA key size | 2048bit |
| Last modified | 2014/01/13 00:00 |

Close

- When the [Delete] button is clicked, the installed server certificate will be deleted.
- When “HTTPS” is selected for “Connection”, it is impossible to delete the server certificate.
- To change (or update) the server certificate, perform step 1 and 2.

IMPORTANT

- Before deleting the valid server certificate (security certificate), confirm that there is a backup file on the PC or another media. The backup file will be required when installing the server certificate again.
- When the server certificate has expired, the HTTPS function will become unavailable. When the unit is restarted, the connection protocol will be changed to HTTP. Update the server certificate before it expires.
- The expiration date of the server certificate can be checked by double-clicking the server certification file issued by CA.

13.2.5 Configuration of the connection protocol

- Select “HTTP” or “HTTPS” for “Connection” to determine the protocol used to access the unit.
 - HTTP:** Only the HTTP connection is available.
 - HTTPS:** Only the HTTPS connection is available.
- Designate the HTTPS port number to be used for “HTTPS port”.
 - Available port number:** 1 - 65535
 - Default:** 443

The following port numbers are unavailable since they are already in use.
20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 554, 995, 10669, 10670, 52000, 59000 - 61000
- Click the [Set] button.
 - The unit will restart, and it will become possible to access to the units using the HTTPS protocol.
(→page 7, page 14, page 15)

Note

- The unit will restart after the connection setting is changed.
- When using the self-signed certificate:**
If the unit is accessed using the HTTPS protocol for the first time, the warning window will be displayed. In this case, follow the instructions of the wizard to install the self-signed (security) certificate.
(→page 81)

- **When using the server certificate:**
In advance, install the root certificate and intermediate certificate on the browser in use. Follow the instructions of CA for how to obtain and install these certificates.
- When the unit is accessed using the HTTPS protocol, the refresh interval and frame rate of images may be lower.
- When the unit is accessed using the HTTPS protocol, it may take time to display images.
- When the unit is accessed using the HTTPS protocol, the images may be distorted.
- When the unit is accessed using the HTTPS protocol, the number of users that can access the unit may be reduced. The maximum number of concurrent access user varies depending on the maximum image size and transmission format.

13.3 Access the unit using the HTTPS protocol

1. Start up the web browser.
2. Enter the IP address of the unit in the address box of the browser.
 - **Example of entry:** https://192.168.0.10/

IMPORTANT

- When the HTTPS port number is changed from “443”, enter “https://IP address of the unit + : (colon) + port number” in the address box of the browser.
(**Example:** https://192.168.0.11:61443)
 - When the unit is in a local network, configure the proxy server setting of the web browser (under [Internet Options...] under [Tools] of the menu bar) to bypass the proxy server for the local address.
3. Press the [Enter] key on the keyboard.
 - The “Live” page will be displayed.
 - When the security alert window is displayed, install the security certificate. (→page 82 - page 88)
 - When “On” is selected for “User auth.”, the authentication window will be displayed before displaying live images for the user name and password entries.

IMPORTANT

- When the unit is accessed using the HTTPS protocol, the refresh interval and frame rate of images may be lower.

13.3.1 Install the security certificate

When the security certificate of the unit to access is not installed on the PC, the security alert window will be displayed each time the unit is accessed using the HTTPS protocol. To have the security alert window not displayed, it is necessary to install the security certificate in the following procedure. If the certificate is not installed, the alert window will be displayed each time the unit is accessed.

Note

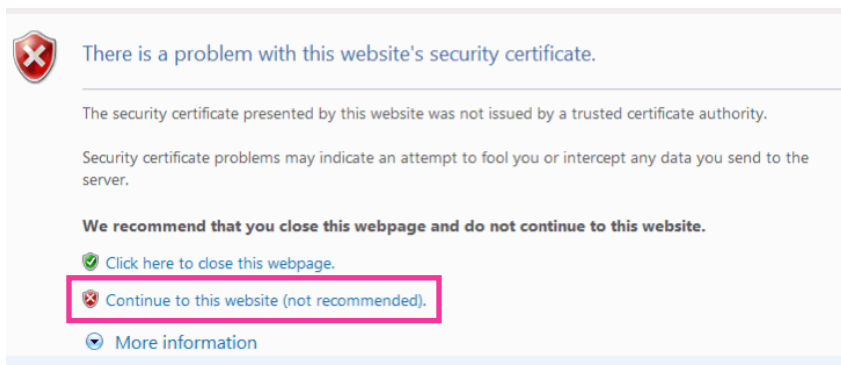
- The security certificate is installed on the PC with the information registered for “Common Name”. Therefore, the information registered for “Common Name” must be same as the address or host name for the unit access. If the certificate is not the same, the security alert window will be displayed each time the unit is accessed.
- When the address or host name of the unit is changed, the security alert window will be displayed each time the unit is accessed even if the security certificate is installed. Install the security certificate again.
- When the unit access is open to the Internet, enter the address name or host name to access via the Internet for “Common Name”. In this case, the security alert window will be displayed each time the unit is locally accessed, even if the security certificate is installed.

- When the security certificate is properly installed, a key icon is displayed in the address box of the web browser that has accessed the unit. (When using Internet Explorer 7, Internet Explorer 8, or Internet Explorer 9)

When using Internet Explorer 7, Internet Explorer 8, or Internet Explorer 9

When using Internet Explorer 7 or Internet Explorer 8 with Windows XP, note that some of the displayed windows may differ from the following descriptions.

1. Access the unit using the HTTPS protocol.
2. When the security alert window is displayed, click “Continue to this website (not recommended).”

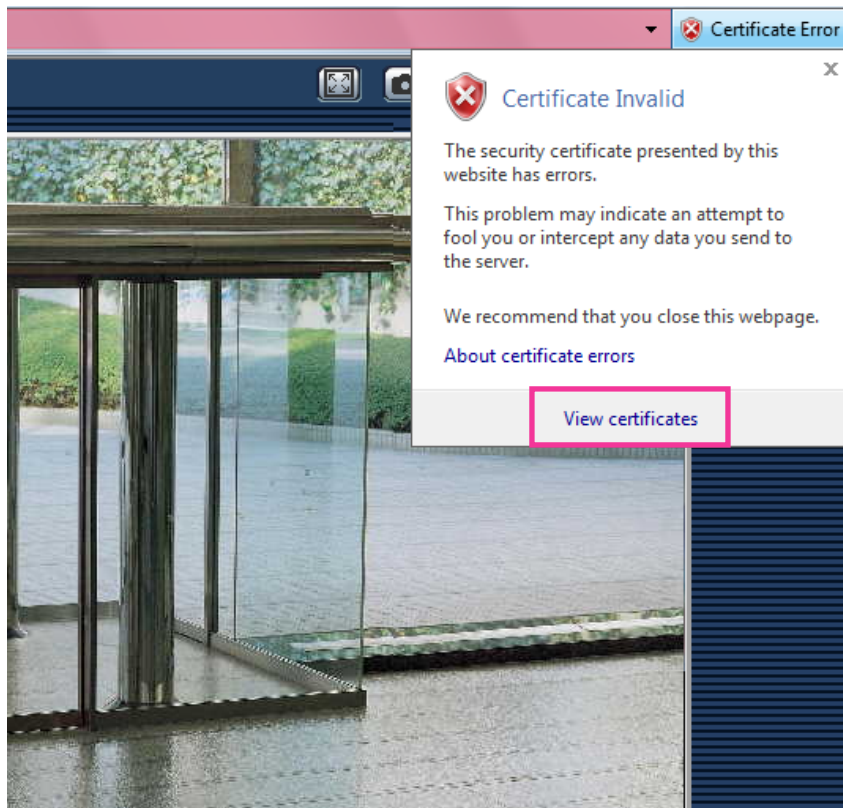


→ The “Live” page will be displayed. If an authentication window is displayed, enter the user name and password.

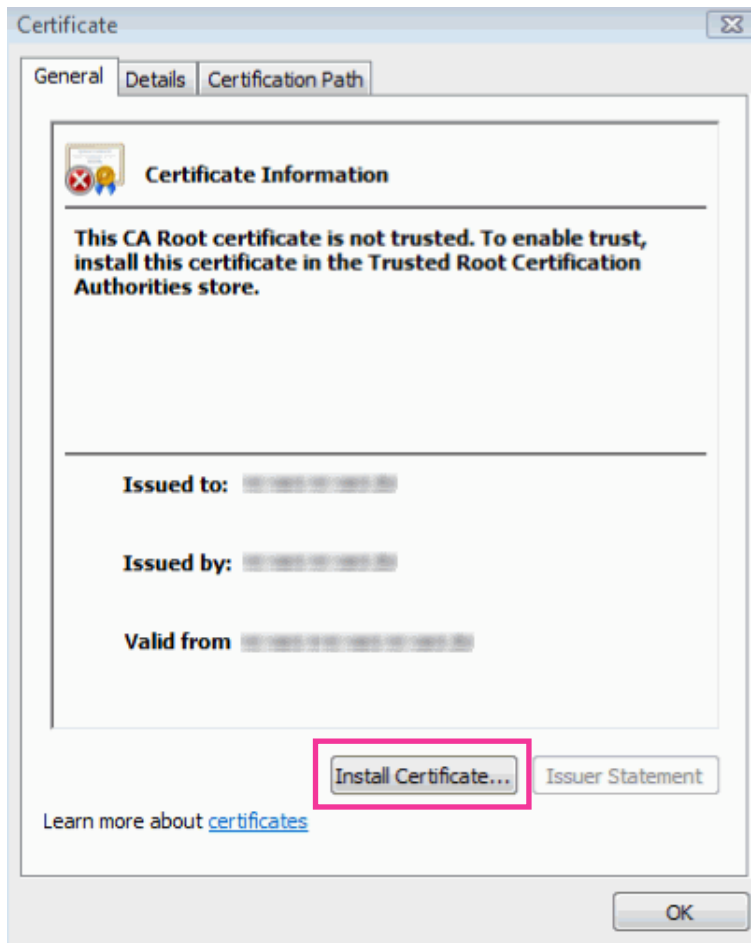
Note

- If this window is displayed when accessing a device other than the unit or a website, a security problem may have occurred. In this case, check the system status.

3. Click “Certificate Error” over the URL, and click “View certificates”.



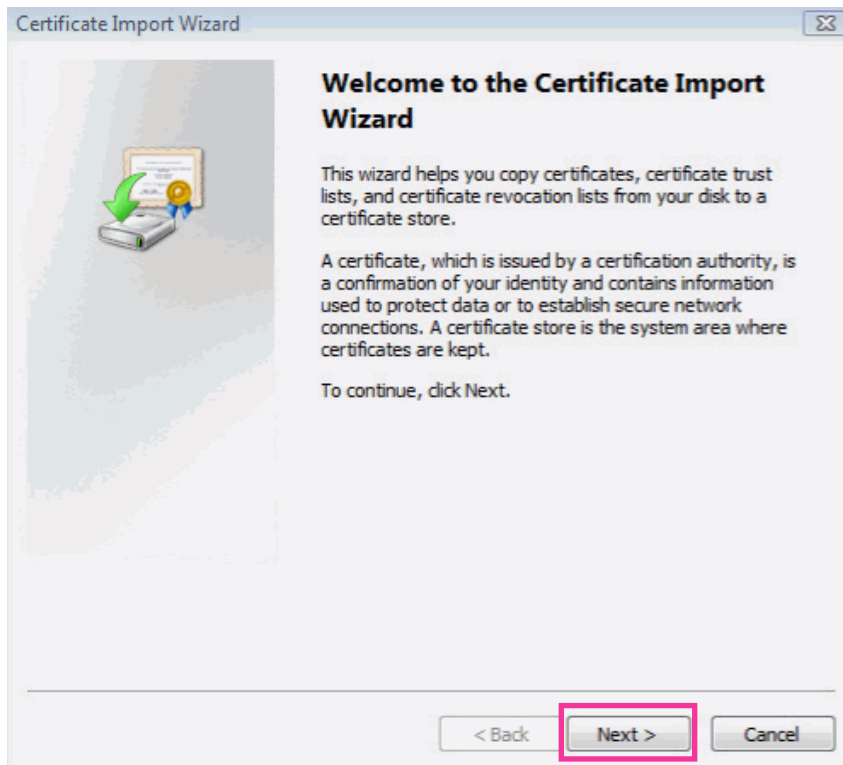
4. Click "Install Certificate...".



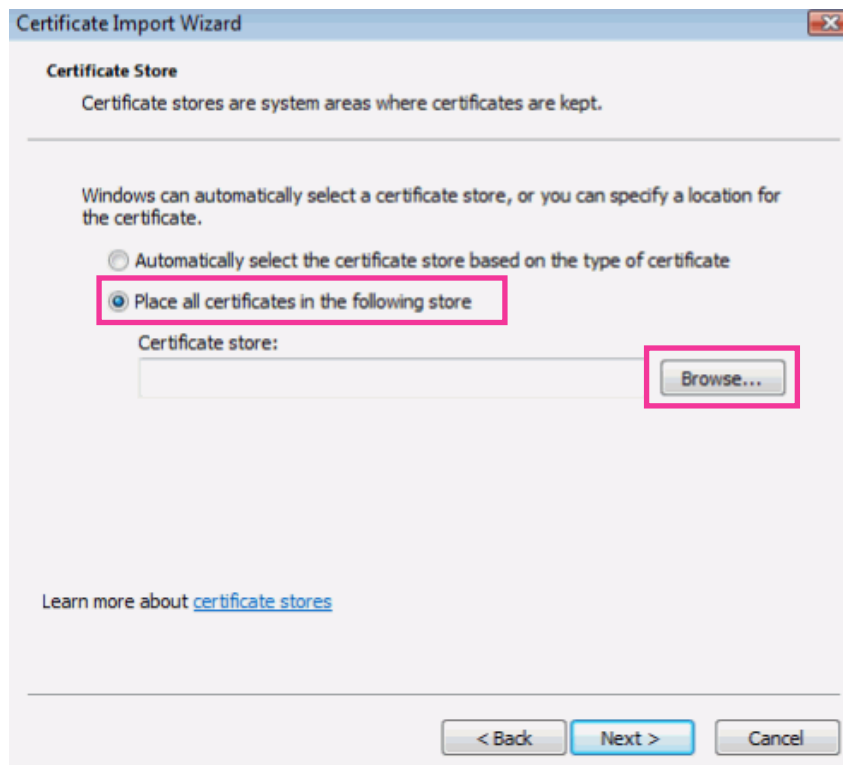
Note

- If [Install Certificate...] is not displayed, close Internet Explorer once, and select [Run as Administrator] to launch Internet Explorer again. Click [Start] → [All Programs] → right click [Internet Explorer] → click [Run as Administrator].

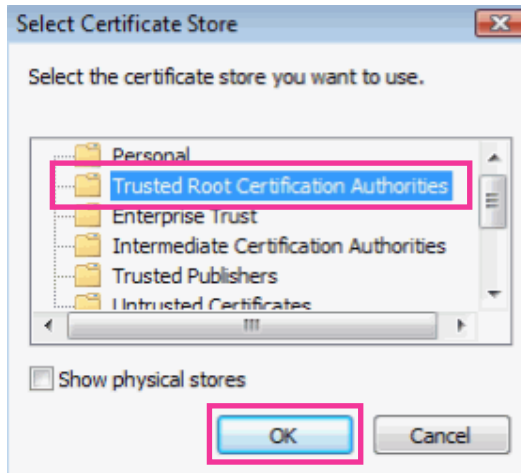
5. Click “Next” displayed on “Certificate Import Wizard”.



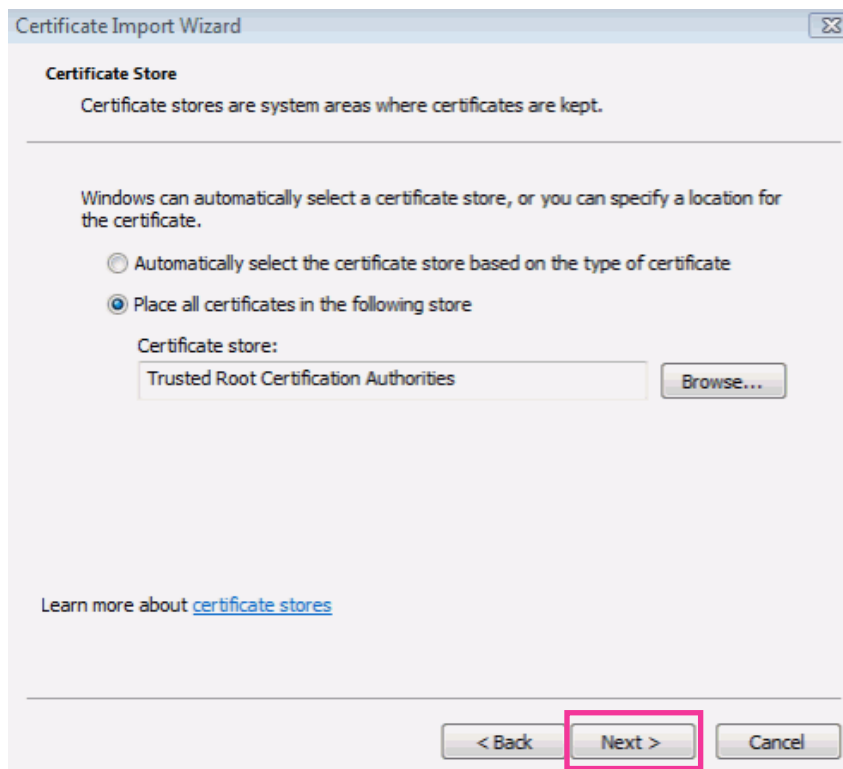
6. Select “Place all certificates in the following store”, and click “Browse...”.



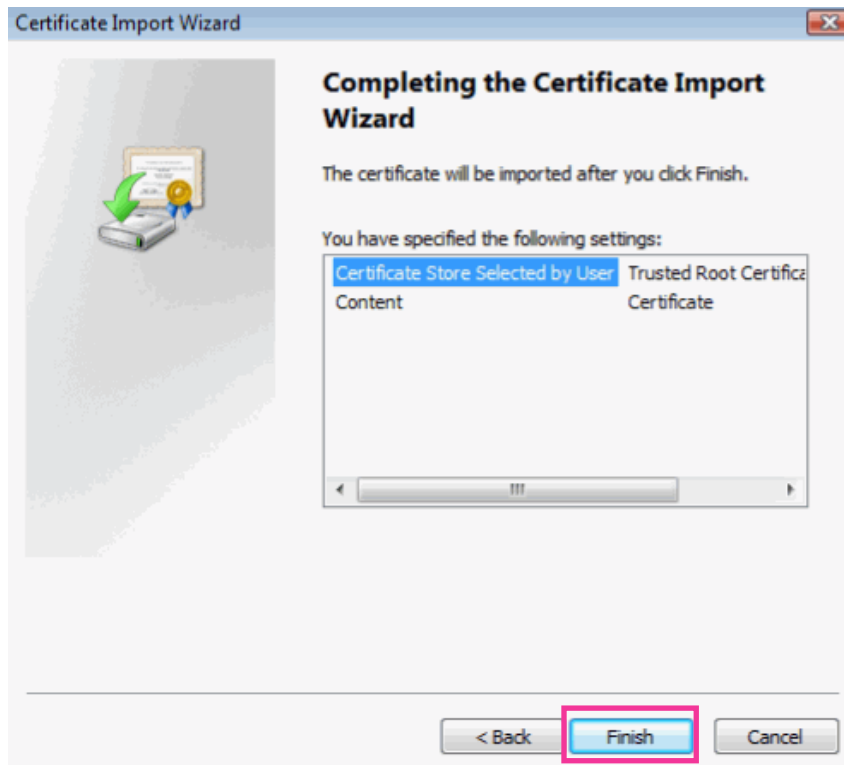
7. Select “Trusted Root Certificate Authorities”, and click “OK”.



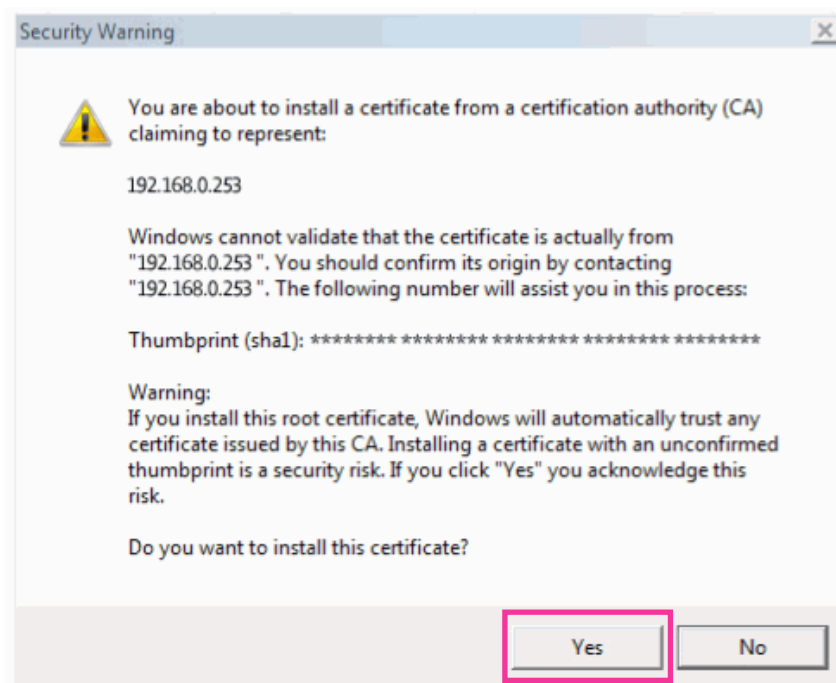
8. Click “Next”.



9. Click "Finish".

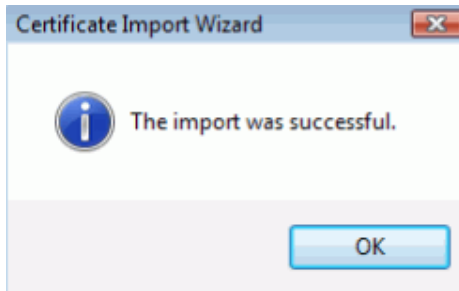


10. Click "Yes".



→ When the import is successfully completed, the screen "The import was successful." will be displayed.

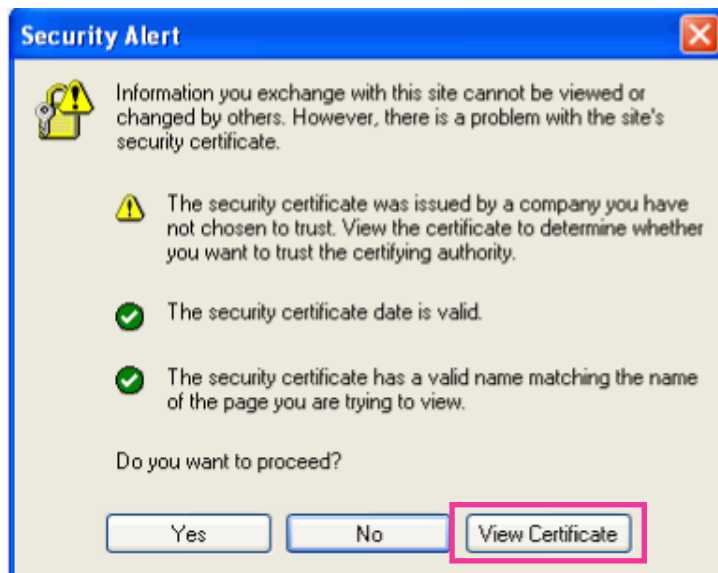
11. Click "OK".



→ When the browser is restarted after the certificate is imported, "Certificate Error" will not be displayed.

OS: Windows XP, Web browser: When using Internet Explorer 6

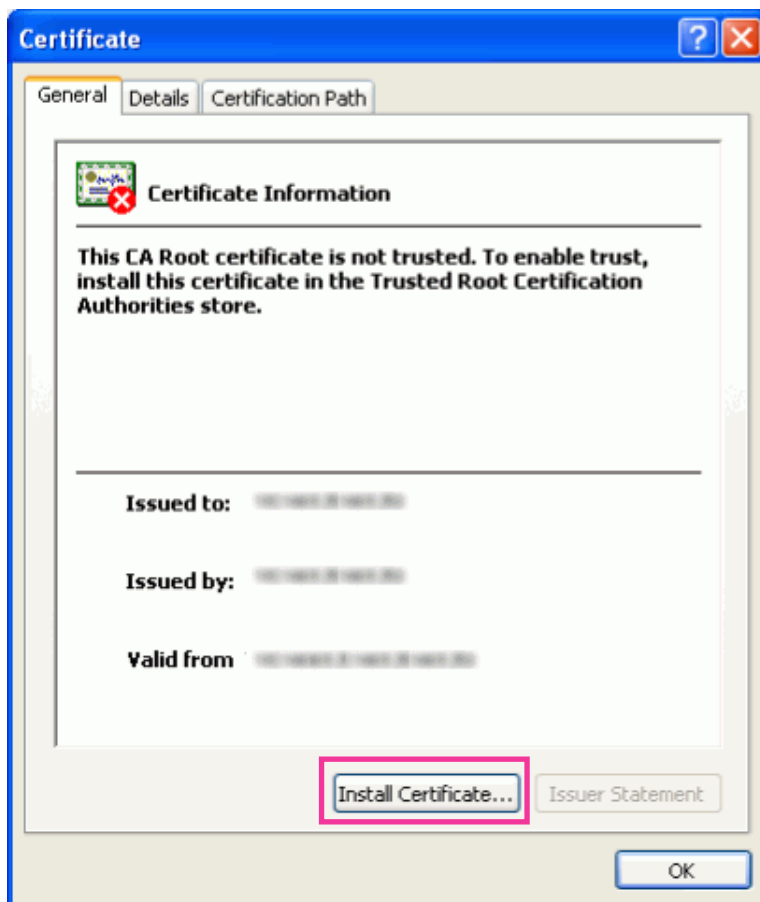
1. Access the unit using the HTTPS protocol.
2. Click "View Certificate".



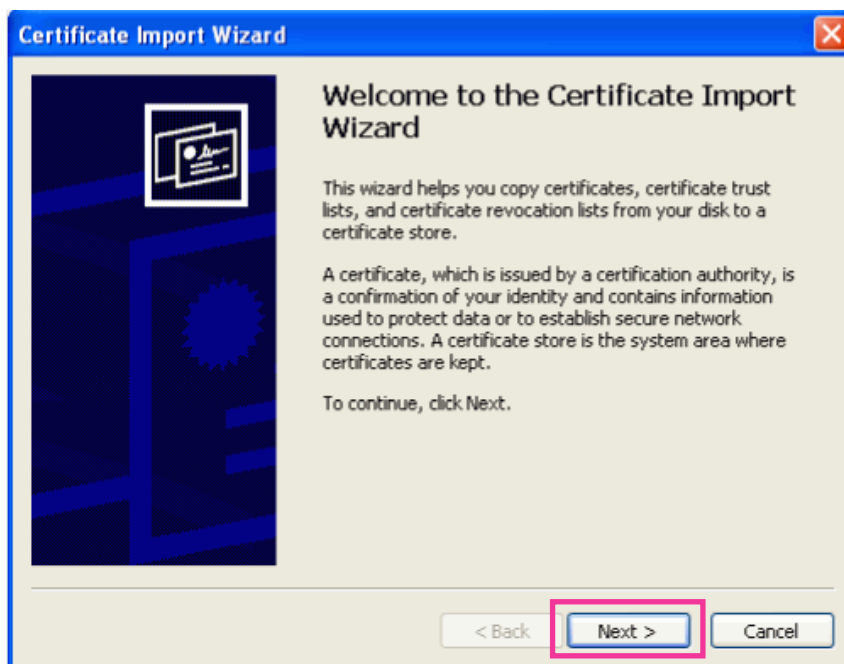
Note

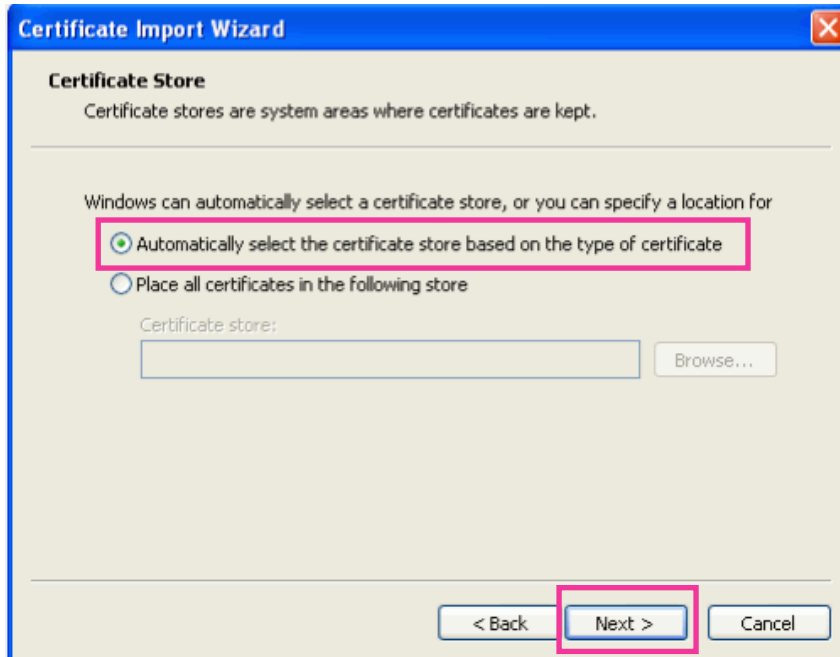
- If this window is displayed when accessing a device other than the unit or a website, a security problem may have occurred. In this case, check the system status.

3. Click “Install Certificate...”.

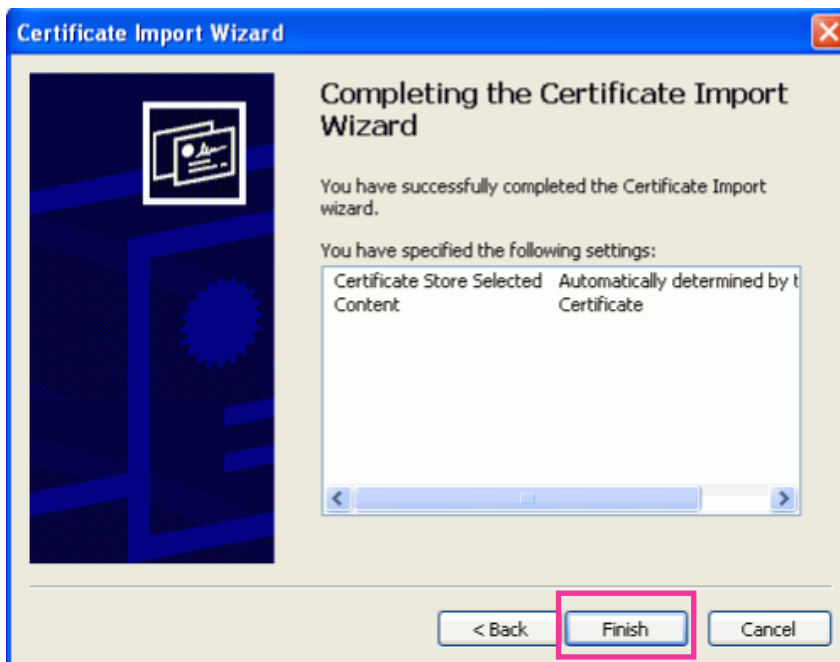


4. Click “Next” according to the procedures displayed on the displayed on “Certificate Import Wizard”.

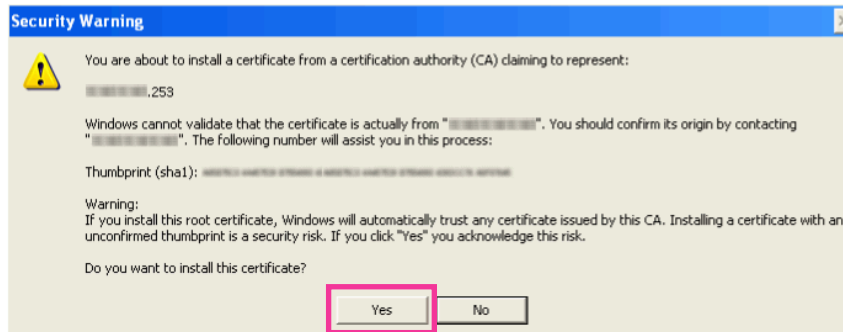




5. Click "Finish".



6. When the security alert window is displayed, click “Yes”.



→ When the import is successfully completed, the screen “The import was successful.” will be displayed.

7. Click “OK”.



→ When the browser is restarted after the certificate is imported, “Certificate Error” will not be displayed.

13.4 Configure the settings relating to DDNS [DDNS]

Click the [DDNS] tab on the “Network” page. (→page 21, page 23)

To access this unit via the Internet, it is necessary to configure the settings for the DDNS function.

When activating the DDNS function using the camera, either of the following DDNS services is available.

- “Viewnetcam.com” service
- Dynamic DNS Update (RFC2136 compliant)

IMPORTANT

- Before using the DDNS service, it is necessary to perform the port forwarding setting for the router.
- **About Dynamic DNS Update (RFC2136 compliant)**
Operation using DDNS services other than the “Viewnetcam.com” service is not guaranteed. We are not responsible for any troubles or accidents on the circumstances where the unit is used arising out of such services.
Refer to the DDNS service providers for the selection and configuration of the DDNS services other than the “Viewnetcam.com” service.

Note

- “Viewnetcam.com” is a Dynamic DNS service designed for use with Panasonic Network Cameras. Refer to the “Viewnetcam.com” website (<http://www.viewnetcam.com/>) for further information about the service.

About DDNS services (IPv4/IPv6)

By using a DDNS service, it becomes possible to view camera images via the Internet.

The DDNS service associates dynamic global addresses and domain names.

It is possible to configure the settings for the “Viewnetcam.com” or Dynamic DNS Update (RFC2136 compliant). In most of the DNS services offered by providers, global addresses are not static but dynamic. Therefore, access to the unit via an old global address may be invalidated after a certain period of time. Either of the following services is required when accessing a unit whose global address is not static via the Internet.

- **DDNS service (such as “Viewnetcam.com”)**

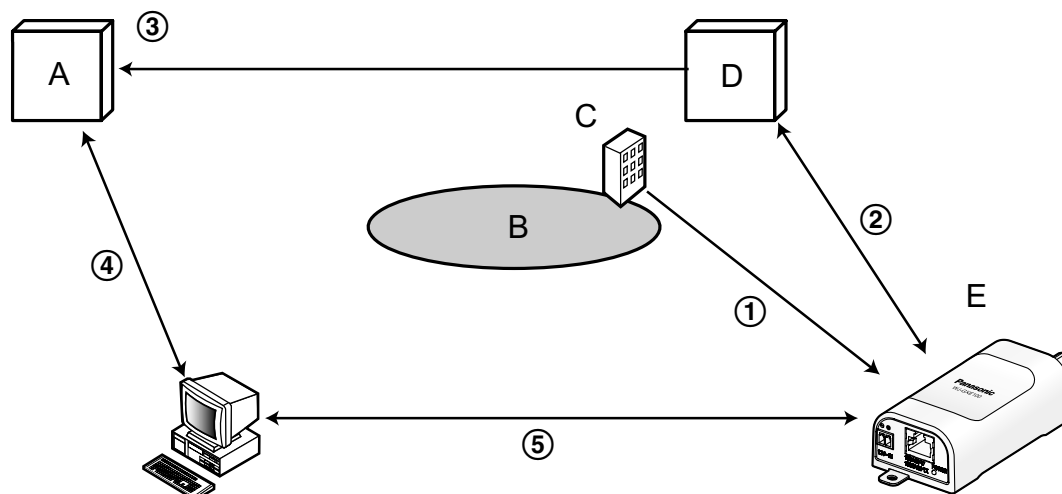
It is possible to access via a registered and static domain name (example: *****.viewnetcam.com) even after the global address is changed. Enrollment in a domain name service is required even when using the IPv6 connection.

Refer to the “Viewnetcam.com” website (<http://www.viewnetcam.com/>) for further information about the service.

- **Static IP address service (such as a service offered by a contracted provider)**

In this service, global addresses are static (not changed).

13.4.1 Configuration of the DDNS service (Example of the “Viewnetcam.com” service)



- A. DNS server
- B. Internet
- C. Provider
- D. “Viewnetcam.com” service server
- E. Remote site

① **Global address is changed.**

The contracted provider allocates a global address to the router (or the unit). The global address is not static but dynamic.

② **“*****.viewnetcam.com” and the current global address is automatically registered.**

If you are enrolled in “Viewnetcam.com”, the unique “domain name” (example: *****.viewnetcam.com) will be allocated. The “Viewnetcam.com” service server automatically manages the domain name of unit and the global address of router (or unit) when a unit automatically notifies the service server of the global address.

③ **Current global address is automatically registered via “*****.viewnetcam.com”.**

The “Viewnetcam.com” service server registers the global address and the domain name of router (or unit) in the DNS server.

④ **Global address is obtained via the URL (domain name).**

By entering the URL (including the domain name) on the web browser when accessing the unit via the Internet, the DNS server identifies the registered global address of router (or unit).

⑤ **Access using the current global address**

The identified global address is used for accessing the router (or unit) to monitor images.

Note

- Refer to the contracted provider whether the current IP address is static or not.
- Depending on the provider, local addresses may be allocated. In this case, the DDNS service is unavailable. Refer to the contract provider for further information.

**[DDNS]**

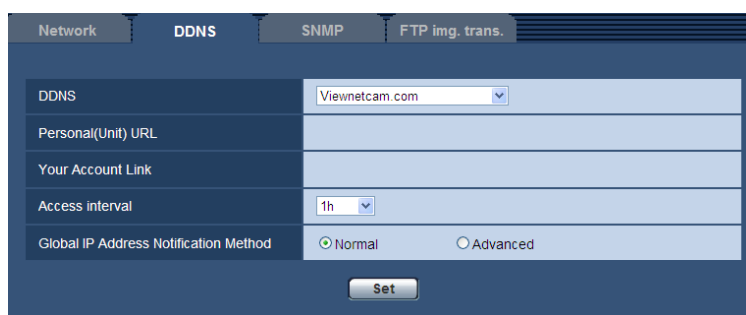
Select the DDNS service to determine whether or not to use DDNS.

- **Off:** Does not use the DDNS function.
- **Viewnetcam.com:** Uses the “Viewnetcam.com” service.
- **Dynamic DNS Update:** Uses Dynamic DNS Update (RFC2136 compliant) without the DHCP cooperation.
- **Dynamic DNS Update(DHCP):** Uses Dynamic DNS Update (RFC2136 compliant) with the DHCP cooperation.
- **Default:** Off

Note

- When using Dynamic DNS Update (RFC2136 compliant), refer to the network administrator for whether or not to cooperate with the DHCP.

13.4.2 When using the “Viewnetcam.com” service

**[Personal(Unit) URL]**

The URL of the unit registered for “Viewnetcam.com”.

[Your Account Link]

When the displayed URL is clicked, the registration window for the “Viewnetcam.com” service will be displayed in a newly opened window.

Register the information in the registration window to enroll in the “Viewnetcam.com” service.

[Access interval]

Select the interval to access the “Viewnetcam.com” service server to check the IP address and the host name from the following.

10min/ 20min/ 30min/ 40min/ 50min/ 1h

- **Default:** 1h

[Global IP Address Notification Method]

Typically [Global IP Address Notification Method] should be set to “Normal”.

If you cannot access the unit using the registered URL 30 minutes after registering with “Viewnetcam.com”, select “Advanced”.

In this case, UPnP (→page 70) must be enabled for the unit and for the router.

- **Default:** Normal

13.4.3 Procedure to register information for the “Viewnetcam.com” service

There are 2 methods to configure the “Viewnetcam.com” service.

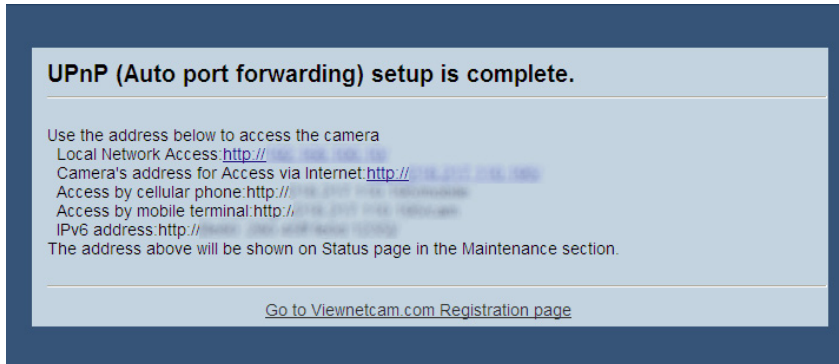
- **Configure from the [Internet] tab of the “Basic” page:**
“UPnP (Auto port forwarding)” and “Viewnetcam.com” can both be configured on the [Internet] tab.
- **Configure from the [DDNS] tab of the “Network” page:**
Only “Viewnetcam.com” can be configured on the [DDNS] tab.

Configuring from the [Internet] tab of the “Basic” page

1. Click the [Internet] tab of the “Basic” page.
2. Select “On” for “UPnP (Auto port forwarding)”, and select “Viewnetcam.com” for “DDNS”, then click [Set].

The screenshot shows the 'Basic' configuration page with the 'Internet' tab selected. The 'UPnP(Auto port forwarding)' option is set to 'On'. The 'DDNS' dropdown menu is set to 'Viewnetcam.com'. Below the dropdown, there is explanatory text: 'To allow access to the camera from the Internet, activate the auto port forwarding (IPv4) setting and register on the DDNS service "Viewnetcam.com" (free). Note: The camera may be accessed from a third party if the Internet access is allowed.' A 'Set' button is located below the text. At the bottom, there is a section for 'Recommended network setting for internet' with a message 'A setup suitable for internet environment is carried out.' and another 'Set' button.

3. When "UPnP (Auto port forwarding) setup is complete." is displayed, click "Go to Viewnetcam.com Registration page".
→ The registration window for "Viewnetcam.com" will be displayed in a newly opened window.

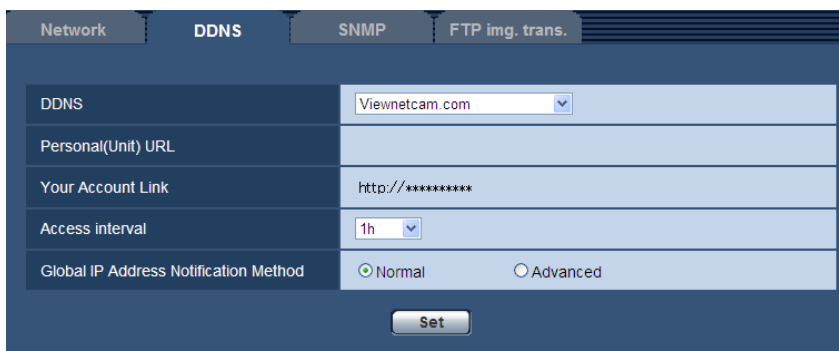


Refer to step 3 of "Configuring from the [DDNS] tab of the "Network" page" for the required settings.

Configuring from the [DDNS] tab of the "Network" page

Select "On" for "Auto port forwarding" of the UPnP function on the [Network] tab of the "Network" page, and then complete the port forwarding settings for the router. (→page 70) After this, register the information for the "Viewnetcam.com" service in the following steps.

1. Select [Viewnetcam.com] for [DDNS] and click the [Set] button.
→ A URL is displayed in [Your Account Link].
If a URL is not displayed in [Your Account Link], confirm the unit's network settings and Internet connection, then click [Set] again.
2. Click the URL displayed in [Your Account Link].



- The registration window for "Viewnetcam.com" will be displayed in a newly opened window.
When the registration window is not displayed, check that the PC is being connected to the Internet, and click the reload button of the browser.
3. Register the information for "Viewnetcam.com" by following the instructions of the wizard.
→ When the message "The new camera is successfully registered to Viewnetcam.com" is displayed, close the registration window.

13 Configuring the network settings [Network]

The URL set at the time of registration can be used for unit access. However, this URL is unavailable when accessing the unit from the PC connected to the same network (LAN).

| Network | DDNS | SNMP | FTP img. trans. |
|---------------------------------------|--|------|-----------------|
| DDNS | | | |
| DDNS | Viewnetcam.com | | |
| Personal(Unit) URL | ***** | | |
| Your Account Link | http://***** | | |
| Access Interval | 1h | | |
| Global IP Address Notification Method | <input checked="" type="radio"/> Normal <input type="radio"/> Advanced | | |
| <div>Set</div> | | | |

Note

- When the registration for the “Viewnetcam.com” service is completed, the URL registered for “Personal(Unit) URL” is displayed. It may take up to about 30 minutes until the URL of the registered unit is validated.
- To cancel the enrollment in the “Viewnetcam.com” service, access the “Viewnetcam.com” website (<http://www.viewnetcam.com/>) later.
- When “Expired” is displayed in the URL of “Viewnetcam.com” in the viewnetcam settings page or the status page, restart the unit after registering the “Viewnetcam.com” service. After restarting the unit, check that the registered URL is displayed in the URL of “Viewnetcam.com” of [Status] - [Viewnetcam.com] on the “Maintenance” page.
- It is possible to check the information registered for the “Viewnetcam.com” service by accessing the URL displayed beside “Your Account Link”. When the URL is not displayed, check that the PC is being connected to the Internet, and click the [Set] button.
- If access often fails due to the change in the global address of router, set a smaller value for “Access interval”.
- If images are not correctly displayed, click [Set] for “Recommended network setting for internet” on the [Internet] tab of the “Basic” page.

Configuring port forwarding when not using UPnP

When using a router that does not support UPnP, port forwarding must be manually configured for the router.

1. Click the [Network] tab of the “Network” page.
2. Select “Static” for “Network Settings”.
3. Confirm the IP address, port number, and other information displayed here, and change the settings as necessary. (This information is required when configuring port forwarding on the router.)
4. Click the [Set] button.
5. Refer to the manuals provided with the router when configuring port forwarding on the router.
 - When configuring port forwarding on the router, use the IP address and port number information confirmed in step 3.
 - The port forwarding function may also be called “Address translation”, “Static IP masquerade”, “Virtual server”, or “Port mapping” depending on the router used.

Note

- When manually configuring port forwarding on the router, make sure to select “Off” for “Auto port forwarding”.

13.4.4 Checking the information registered for the “Viewnetcam.com” service

It is possible to check if the unit has been registered for the “Viewnetcam.com” service. (→page 108)

13.4.5 When using “Dynamic DNS Update”

The screenshot shows the DDNS configuration interface. At the top, there are tabs for 'Network', 'DDNS', 'SNMP', and 'FTP img. trans.'. The 'DDNS' tab is active. Below the tabs, there is a dropdown menu for 'DDNS' with 'Dynamic DNS Update' selected. Below this is a text input field for 'Host name' which is currently empty. Below that is a dropdown menu for 'Access interval' with '24h' selected. At the bottom right of the form is a 'Set' button.

[Host name]

Enter the host name to be used for the Dynamic DNS Update service.

- **Available number of characters:** 3 - 250 characters
Enter in the form of “(host name). (domain name)”.
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

Note

- Refer to the network administrator for further information about the available host names.

[Access interval]

Select the interval to access the Dynamic DNS Update service server to check the IP address and the host name from the following.

10min/ 20min/ 30min/ 40min/ 50min/ 1h/ 6h/ 24h

- **Default:** 24h

13.4.6 When using “Dynamic DNS Update(DHCP)”

The screenshot shows the DDNS configuration interface. At the top, there are tabs for 'Network', 'DDNS', 'SNMP', and 'FTP img. trans.'. The 'DDNS' tab is active. Below the tabs, there is a dropdown menu for 'DDNS' with 'Dynamic DNS Update(DHCP)' selected. Below this is a text input field for 'Host name' which is currently empty. At the bottom right of the form is a 'Set' button.

[Host name]

Enter the host name to be used for the Dynamic DNS Update service.

- **Available number of characters:** 3 - 250 characters
Enter in the form of “(host name). (domain name)”.
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).

- **Default:** None (blank)

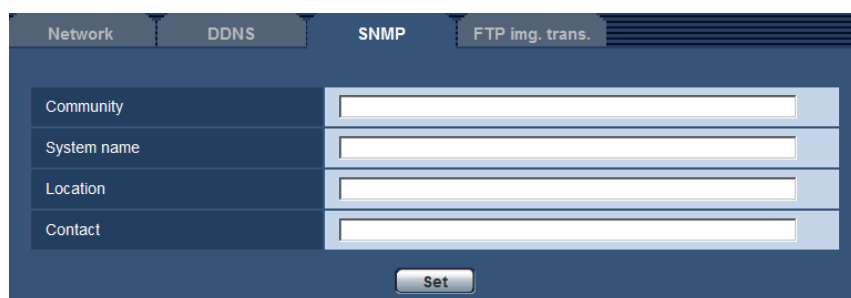
Note

- Refer to the network administrator for further information about the available host names.

13.5 Configure the settings relating to SNMP [SNMP]

Click the [SNMP] tab on the “Network” page. (→page 21, page 23)

The settings relating to SNMP can be configured on this page. It is possible to check the status of the unit by connecting to the SNMP manager. When using the SNMP function, contact the network administrator.



The screenshot shows a web interface for configuring network settings. At the top, there are four tabs: "Network", "DDNS", "SNMP", and "FTP img. trans.". The "SNMP" tab is currently selected. Below the tabs, there are four input fields with labels: "Community", "System name", "Location", and "Contact". Each field is a text box with a light blue border. At the bottom right of the form, there is a "Set" button.

[Community]

Enter the community name to be monitored.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

IMPORTANT

- When using the SNMP function, it is necessary to enter the community name. When no community name is entered, the SNMP function will not work.

[System name]

Enter a system name to be used to manage the unit with the SNMP function.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

[Location]

Enter the name of the location where the unit is installed.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

[Contact]

Enter the E-mail address or the phone number of the SNMP manager.

- **Available number of characters:** 0 - 255 characters
- **Default:** None (blank)

13.6 Configure the settings relating to the FTP periodic image transmission [FTP img. trans.]

Click the [FTP img. trans.] tab on the “Network” page. (→page 21, page 23)

The settings relating to the periodic transmission of images to an FTP server can be configured on this page. To transmit images to an FTP server periodically, it is necessary to configure the settings of the FTP server in advance (→page 62). Refer to page 100 for descriptions of how to configure schedules of image transmission.

IMPORTANT

- When “D1” is selected for “Picture (Camera) mode”, the FTP periodic image transmission will not be possible.
- Depending on the network line speed or the network traffic, images may not be transmitted at the exact designated interval or period.
- When “On” is selected for both of the alarm image transmission function and the FTP periodic image transmission function, the alarm image transmission function will be given priority over the FTP periodic image transmission function. For this reason, images may not be transmitted at the exact designated interval or period if alarms occur frequently.

FTP periodic image transmission

[FTP >>]

When “FTP >>” is clicked, the [FTP] tab of the “Server” page will be displayed. (→page 62)

[FTP periodic image transmission]

Select “On” or “Off” to determine whether or not to transmit images using the FTP periodic image transmission function.

When “On” is selected, it is necessary to configure the settings of the FTP server. (→page 62)

- **Default:** Off

[Directory name]

Enter the directory name where the images are to be saved.

For example, enter “/img” to designate the directory “img” under the root directory of the FTP server.

- **Available number of characters:** 1 - 256 characters
- **Unavailable characters:** " & ;
- **Default:** None (blank)

[File name]

Enter the file name (name of the image file to be transmitted) and select the naming option from the following.

- **Name w/time&date:** File name will be ["Entered file name" + "Time and date (year/ month/ day/ hour/ minute/ second)" + "Serial number (starting from 00)"].
- **Name w/o time&date:** File name will be the characters entered for "File name" only. When "Name w/o time&date" is selected, the file will be overwritten each time a file is newly transmitted.
- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & ; : / * < > ? \ |
- **Default:** None (blank)

Note

- When "Name w/time&date" is selected, the file name will be ["Entered file name" + "Time and date (year/ month/ day/ hour/ minute/ second)" + "Serial number (starting from 00)"] + "s" during summer time.

[Transmission interval]

Select the interval for the FTP periodic image transmission from the following.

1s/ 2s/ 3s/ 4s/ 5s/ 6s/ 10s/ 15s/ 20s/ 30s/ 1min/ 2min/ 3min/ 4min/ 5min/ 6min/ 10min/ 15min/ 20min/ 30min/ 1h/ 1.5h/ 2h/ 3h/ 4h/ 6h/ 12h/ 24h

- **Default:** 1s

[Image capture size]

Select the capture size of images to be transmitted from the following.

| | |
|----------------------------------|-----------------|
| Picture (Camera) mode VGA [4:3] | QVGA/VGA |
| Picture (Camera) mode VGA [16:9] | 320x180/640x360 |

- **Default:** VGA

13.7 Configure the schedule settings of the FTP periodic image transmission [FTP img. trans.]

Click the [FTP img. trans.] tab on the "Network" page. (→page 21, page 23)

The schedule settings of the FTP periodic image transmission can be configured in this section. Refer to page 99 for further information about the settings relating to the FTP periodic image transmission.

IMPORTANT

- When "D1" is selected for "Picture (Camera) mode", the schedule settings of the FTP periodic image transmission are unavailable.

13.7.1 How to set the schedules

FTP image transmission schedule

| | |
|------------|--|
| Schedule 1 | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun <input type="checkbox"/> 24h 00 : 00 - 00 : 00 |
| Schedule 2 | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun <input type="checkbox"/> 24h 00 : 00 - 00 : 00 |
| Schedule 3 | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun <input type="checkbox"/> 24h 00 : 00 - 00 : 00 |

Set

| | 0:00 | 6:00 | 12:00 | 18:00 | 24:00 |
|-----|------|------|-------|-------|-------|
| Mon | | | | | |
| Tue | | | | | |
| Wed | | | | | |
| Thu | | | | | |
| Fri | | | | | |
| Sat | | | | | |
| Sun | | | | | |

1. Check the check box of the desired day of the week of "FTP image transmission schedule".
→ The selected day of the week will be validated for the schedule.
2. To designate time, select the desired "hour" and "minute" from the pull-down menu.
When not designating time, check the checkbox of "24h".
3. Click the [Set] button after completing the settings.
→ The result will be displayed at the bottom of the window.

FTP image transmission schedule

| | |
|------------|---|
| Schedule 1 | <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun <input type="checkbox"/> 24h 09 : 00 - 17 : 30 |
| Schedule 2 | <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun <input type="checkbox"/> 24h 23 : 00 - 07 : 00 |
| Schedule 3 | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> 24h 00 : 00 - 00 : 00 |

Set

| | 0:00 | 6:00 | 12:00 | 18:00 | 24:00 |
|-----|------|------|-------|-------|-------|
| Mon | | | | | |
| Tue | | | | | |
| Wed | | | | | |
| Thu | | | | | |
| Fri | | | | | |
| Sat | | | | | |
| Sun | | | | | |

13.7.2 How to delete the set schedule

FTP image transmission schedule

Schedule 1

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Sun

☐ 24h

0900

 -

1730

Schedule 2

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

☐ 24h

2300

 -

0700

Schedule 3

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat ☒ Sun

☒ 24h

0000

 -

0000

Set

| | 0:00 | 6:00 | 12:00 | 18:00 | 24:00 |
|-----|------|------|-------|-------|-------|
| Mon | | | | | |
| Tue | | | | | |
| Wed | | | | | |
| Thu | | | | | |
| Fri | | | | | |
| Sat | | | | | |
| Sun | | | | | |

1. Uncheck the check box of the set day of the week.

2. Click the [Set] button after completing the settings.
→ The schedule of the selected day of the week is deleted.

FTP image transmission schedule

Schedule 1

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☐ 24h

0000

 -

0000

Schedule 2

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☐ 24h

0000

 -

0000

Schedule 3

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☐ 24h

0000

 -

0000

Set

| | 0:00 | 6:00 | 12:00 | 18:00 | 24:00 |
|-----|------|------|-------|-------|-------|
| Mon | | | | | |
| Tue | | | | | |
| Wed | | | | | |
| Thu | | | | | |
| Fri | | | | | |
| Sat | | | | | |
| Sun | | | | | |

102 | Operating Instructions

14 Configure the settings relating to the schedules [Schedule]

On the “Schedule” page, it is possible to configure the settings relating to schedules as follows.

- VMD permission (Video motion detection will be active only in the specified schedule.)
- Access permission (Access to the unit will be allowed only in the specified schedule.)

The “Schedule” page has only the [Schedule] tab.

14 Configure the settings relating to the schedules [Schedule]

Up to 5 schedules can be set.

The screenshot displays the 'Schedule' configuration page. It features a table with five rows, each representing a schedule (Schedule 1 to Schedule 5). Each row has two main sections: 'Schedule mode' and 'Time range'. The 'Schedule mode' section includes a dropdown menu currently set to 'Off'. The 'Time range' section includes checkboxes for each day of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and a time range selector showing '24h' and '00:00' to '00:00'. A pink rectangular box highlights the 'Schedule mode' dropdown and the 'Time range' section for Schedule 1. Below the table is a 'Set' button. At the bottom of the page is a large empty grid with days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) on the left and time slots (0:00, 6:00, 12:00, 18:00, 24:00) on the top.

| Schedule | Schedule mode | Time range |
|--------------------|---------------|---|
| Schedule 1 (White) | Off | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun 24h 00:00 - 00:00 |
| Schedule 2 (Blue) | Off | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun 24h 00:00 - 00:00 |
| Schedule 3 (Green) | Off | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun 24h 00:00 - 00:00 |
| Schedule 4 (Red) | Off | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun 24h 00:00 - 00:00 |
| Schedule 5 (Black) | Off | <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun 24h 00:00 - 00:00 |

Set

0:00 6:00 12:00 18:00 24:00

Mon

Tue

Wed

Thu

Fri

Sat

Sun

1. Select an action to be assigned to the schedule from "Schedule mode".
"Off" is selected at the default.
 - **Off:** No action will be taken for the respective schedule.
 - **VMD permission:** The video motion detection (VMD) function will be active during the period of the schedule.

- **Access permission:** Users whose access level is set to 2 and 3 on the “User auth.” tab (→page 56) can access the unit only in the period of schedule.

Note

- Select “On” for “User auth.” on the [User auth.] tab of “User mng.” page (→page 56) and “Off” for “Host auth.” on the “Host auth.” page (→page 57) to validate “Access permission”.
2. Select days of a week by checking the respective checkboxes.
 3. From the pull-down menu, select the start time and the end time of the schedule.
When not designating time, check the checkbox of “24h”.
 4. Click the [Set] button after completing the settings.
→ The result will be displayed at the bottom of the window.

Note

- The schedules displayed at the bottom of the window can be identified by colors assigned to each schedule.

15 Maintenance of the unit [Maintenance]

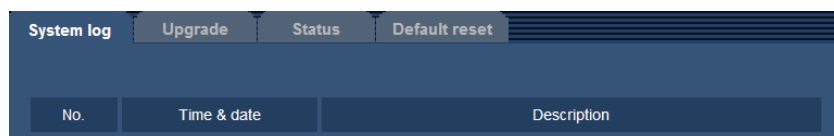
System log check, firmware upgrade, status check and initialization of the setup menu can be performed on this page.

The “Maintenance” page has 4 tabs; the [System log] tab, the [Upgrade] tab, [Status] tab and the [Default reset] tab.

15.1 Check the system log [System log]

Click the [System log] tab of the “Maintenance” page. (→page 21, page 23)

Up to 100 system logs can be saved on the built-in memory of the unit. When the saved system logs have reached the maximum number, the newer logs will overwrite the older system logs. In this case, the oldest log is the first to be overwritten.



| System log | | |
|---------------|-------------|-------------|
| System log | Upgrade | Status |
| Default reset | | |
| No. | Time & date | Description |

[No.]

The serial number of the system log will be displayed.

[Time & date]

Time and date at the error occurrence will be displayed.

Note

- When “Off” is selected for “Time display format” on the [Basic] tab (→page 27), time & date of logs will be displayed in 24-hour format.

[Description]

The descriptions about the system log will be displayed. Refer to page 118 for further information about the system logs.

15.2 Upgrade the firmware [Upgrade]

Click the [Upgrade] tab of the “Maintenance” page. (→page 21, page 23)

The current firmware can be checked and upgraded to the latest version on this page. Contact the dealer for further information about the firmware upgrade.

| System log | | Upgrade | Status | Default reset |
|--------------------------------------|-----------|---------------------------|--------|---------------|
| Model no. | | XXXXXXXXXX | | |
| MAC address | | XX-XX-XX-XX-XX-XX | | |
| Serial no. | | XXXXXXXXXX | | |
| Firmware version | | V1.00 | | |
| IPL version | | V1.00 | | |
| HTML version | | XXXXXXXXXX | | |
| IP address(IPv6) | Linklocal | XXXX:XXXX:XXXX:XXXX::XXXX | | |
| | Static | | | |
| | RA | | | |
| | DHCPv6 | | | |
| Viewer software installation counter | | 0 | | |

☐ Reset the settings to the default after completing the upgrade.
 (Except the network settings)

☒ Do not reset the settings to the default after the upgrade.

Resets to default HTML data after completing the upgrade.

It will take around 8 minutes to complete the upgrade.
Please wait and do not operate the browser during this process.

[Model no.], [MAC address], [Serial no.], [Firmware version], [IPL version], [HTML version], [IP address(IPv6)], [Viewer software installation counter]

Information of each item will be displayed.

1. Download the latest software to the hard disk of the PC from our website (<http://panasonic.net/pss/security/support/info.html>).

IMPORTANT

- A blank (space) cannot be used for the name of the directory where the downloaded firmware to be saved.
2. Click the [Browse...] button and designate the downloaded firmware.
 3. Click the radio button respective to the desired option to determine whether or not to initialize the settings after completing the firmware upgrade.

Note

- Note that the settings cannot be restored after an initialization is operated.
4. Click the [Execute] button.
→ The confirmation window will be displayed.

IMPORTANT

- After completing the upgrade, delete temporary internet files. (→page 122)
- Upgrade the firmware using a PC in the same subnet as the unit.
- Follow the instructions from the dealer when upgrading the firmware.
- When upgrading the application software, use the designated file (extension: img) for the firmware upgrade.
The name of the firmware to be used for the upgrade should be “model name (Use small letters. “WJ-” is not required.)_xxxxx.img”.
* (“xxxxx” indicates the version of the firmware.)
- Do not turn off the power of the unit during the upgrade process.
- Do not perform any operation during upgrading and wait until it completes.
- The following network settings will not be reset when upgrading the firmware after selecting “Reset the settings to the default after completing the upgrade. (Except the network settings)”.
On/Off for DHCP, IP address, subnet mask, default gateway, DNS, primary server address, secondary server address, HTTP port, HTTPS port, connection protocol (HTTP/HTTPS), CRT key, server certificate, UPnP setting, line speed, bandwidth control (bit rate), time & date
- The viewer software used on each PC should be licensed individually. Refer to your dealer for the software licensing.

15.3 Check the status [Status]

Click the [Status] tab of the “Maintenance” page. (→page 21, page 23)

The status of this unit can be checked on this page.

| System log | | Upgrade | | Status | | Default reset | |
|-----------------------|---------------------------------------|---------|--|--------|--|---------------|--|
| Viewnetcam.com | | | | | | | |
| Server | | | | | | | |
| Status | Online | | | | | | |
| Personal(Unit) URL | | | | | | | |
| UPnP | | | | | | | |
| Port number(HTTP) | | | | | | | |
| Status | Online | | | | | | |
| Port number(HTTPS) | | | | | | | |
| Status | Online | | | | | | |
| Router global address | | | | | | | |
| Self check | | | | | | | |
| Hardware1 | 0000-0000-0000-0000-0000-0000-0000-00 | | | | | | |

[Viewnetcam.com]

- **Server:** The URL of the “Viewnetcam.com” service server will be displayed.
- **Status:** The registration status for the “Viewnetcam.com” will be displayed.
- **Personal(Unit) URL:** The URL of the unit registered for “Viewnetcam.com” will be displayed.

[UPnP]

- **Port number(HTTP), Port number(HTTPS):** The port number that is set for UPnP port forwarding will be displayed.
- **Status:** The port forwarding status will be displayed.
- **Router global address:** The global address of router will be displayed.

[Self check]

The self check result of the hardware will be displayed.

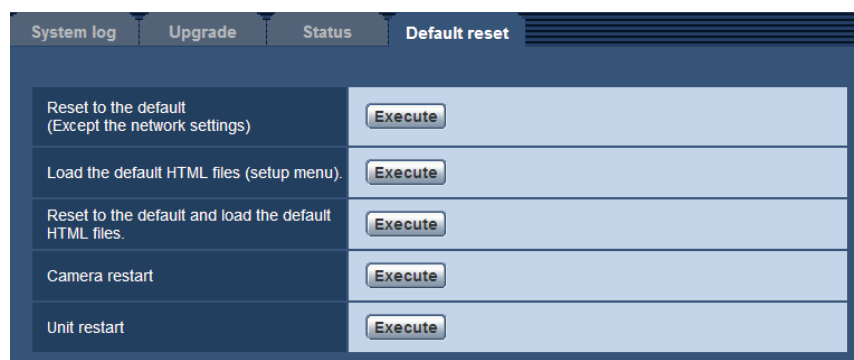
Note

- Refer to our website (<http://panasonic.net/pss/security/support/info.html>) for further information about the contents of the displayed statuses (relating to the "Viewnetcam.com" service, the UPnP function, or the self check).

15.4 Reset the settings/Reboot the unit [Default reset]

Click the [Default reset] tab of the "Maintenance" page. (→page 21, page 23)

The settings and the HTML data of the unit can be initialized and reboot of the camera and unit can be performed on this page.

**[Reset to the default (Except the network settings)]**

Click the [Execute] button to reset the settings to the default. Note that the network settings will not be reset. It is impossible to operate the unit for about 3 minutes after the initialization.

[Load the default HTML files (setup menu).]

Click the [Execute] button to reset the HTML files to the default. It is impossible to operate the unit for about 3 minutes after the initialization.

[Reset to the default and load the default HTML files.]

Click the [Execute] button to reset the settings of the unit and the HTML files to the default. Note that the network settings will not be reset. It is impossible to operate the unit for about 3 minutes after the initialization.

[Camera restart]

Click the [Execute] button to reboot the camera connected to the unit. You will not be able to operate the camera for approximately 1 minute after the reboot.

Because reboot is performed by "RS485 transmission", the RS485 cable must be connected and "On" must be selected for "RS485 transmission". (→page 41)

[Unit restart]

Click the [Execute] button to reboot the unit. It is impossible to operate the unit for about 2 minutes after rebooting the unit.

Note

- To initialize the network settings (→page 66), turn off the power of the unit, then turn on the power again while holding down the INITIAL SET button on the unit, and keep the INITIAL SET button held down for about 5 seconds. Wait about 3 minutes after releasing the button. The unit will start up and the settings including the network settings will be initialized. Do not turn off the power of the unit about 3 minutes after turning on the power.

16 Functional restrictions

16.1 Functional restrictions when “D1” is selected

When “D1” is selected for “Picture (Camera) mode” on the [JPEG/H.264] tab of the “Image” page, the following functions are unavailable.

- FTP periodic image transmission
- Alarm image FTP transmission

17 Number of users that can concurrently access the unit

The maximum number of users that can concurrently access the unit is 14, including users who receive H.264 images and users who receive JPEG images. (When "On" is selected for "Activation" of "Priority stream" on the [System] tab of the "User mng." page.) The number of users that can concurrently access the unit may change according to the network environment and camera settings. Take the following into consideration.

- If "Frame rate" is selected for "Transmission priority" in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab of the "Image" page, the number of users that can concurrently access the unit may be reduced.
- If the setting of "Max bit rate (per client)*" is increased in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab of the "Image" page, the number of users that can concurrently access the unit may be reduced.
- If "Unlimited*" is selected for "Max bit rate (per client)*" in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab of the "Image" page, the number of users that can concurrently access the unit will be limited to 1 user.
- If the "Bandwidth control(bit rate)" on the [Network] tab of the "Network" page is restricted, the number of users that can concurrently access the unit may be reduced.

| Number of users that can concurrently access the unit | Increase | ↔ | Decrease | H.264 connections: about 7 people |
|--|-----------------------------------|---|------------|--------------------------------------|
| "Transmission priority" in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab | Constant bit rate/ Best effort | ↔ | Frame rate | Frame rate |
| "Max bit rate (per client)*" in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab | 64kbps | ↔ | Unlimited* | 1536kbps* |
| "Bandwidth control(bit rate)" on the [Network] tab | Unlimited | ↔ | 64kbps | Unlimited |

Note

- When "Multicast" is selected for "Transmission type" in "H.264(1)" or "H.264(2)" on the [JPEG/H.264] tab of the "Image" page, only the first user who accessed to monitor H.264 images will be included in the maximum number. The second and subsequent users who monitor H.264 images will not be included in the maximum number.
- When "On" is selected for "Activation" of "Priority stream" on the [System] tab of the "User mng." page, because network bandwidth is constantly reserved for "Priority stream", the number of users that can concurrently access the unit may be reduced. When "Off" is selected for "Activation" of "Priority stream", a maximum of 12 users can concurrently access the unit.
- When "HTTPS" is selected for "HTTPS" - "Connection" on the [Network] tab of the "Network" page, the number of users that can concurrently access the unit may be reduced.

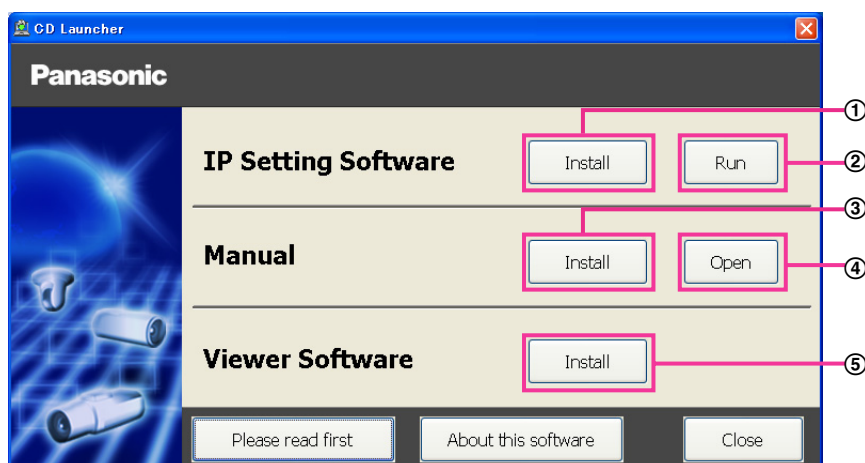
18 Using the CD-ROM

18.1 About the CD launcher

By inserting the provided CD-ROM into the CD-ROM drive of your PC, the CD launcher is automatically started and the license agreement is displayed. Read the agreement and select “I accept the terms in the license agreement”, and then click “OK”.

The CD launcher window is displayed.

- If the launcher window is not displayed, double click the “CDLauncher.exe” file on the CD-ROM.



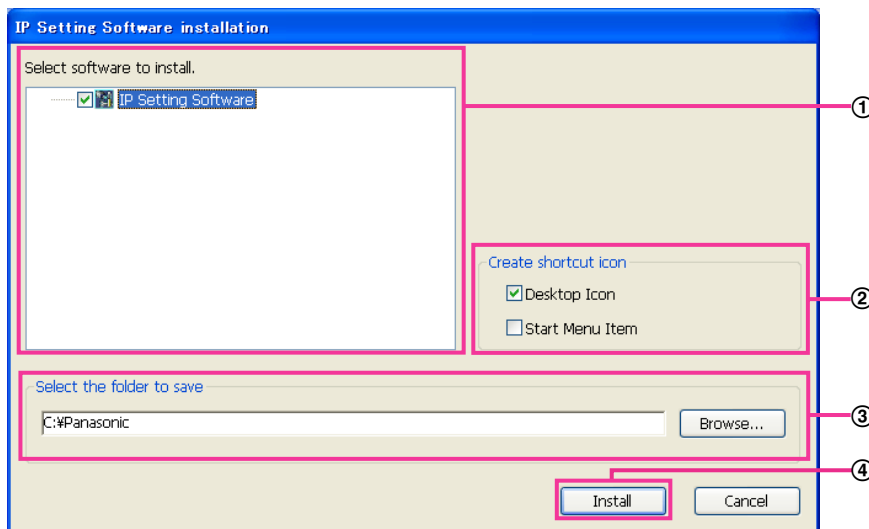
Using the supplied CD-ROM, the following actions can be performed.

- ① The Panasonic “IP Setting Software” can be installed on the PC. (→page 114)
- ② Settings related to the unit’s network can be set from the Panasonic “IP Setting Software”. (→page 116)
- ③ The manuals can be installed on the PC. (→page 115)
- ④ You can also view the manuals without installing them to the PC by clicking the [Open] button.
- ⑤ The Viewer software can be installed on the PC. (→page 115)

Make sure to read the [Readme] file on the provided CD-ROM before using the software.

18.2 Installing Panasonic “IP Setting Software”

On the CD launcher window, click the [Install] button next to [IP Setting Software] to display the Panasonic “IP Setting Software” installation window. Confirm the following settings before starting the installation.



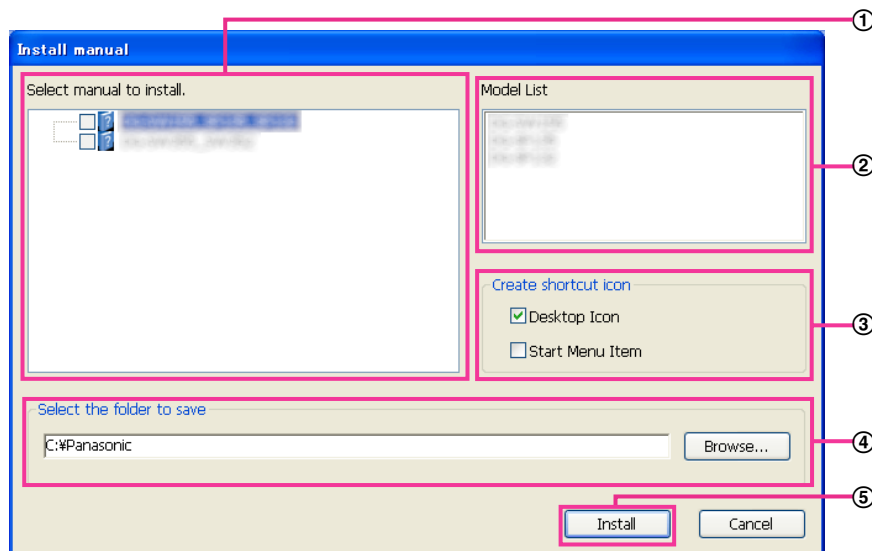
- ① Select the Panasonic “IP Setting Software” to install.
- ② Select where to create the Panasonic IP setting shortcut icon when the Panasonic “IP Setting Software” is installed.
- ③ Specify which folder on the PC to install the Panasonic “IP Setting Software” to.
- ④ Click the [Install] button to start the installation.

Note

- To uninstall the Panasonic “IP Setting Software” delete the shortcut icon from where you specified it to be installed (the default is on the desktop) during installation and the [EasyIPConfig] folder from the folder (the default is C:\Panasonic) you specified during installation.

18.3 Installing the manuals

On the CD launcher window, click the [Install] button next to [Manual] to display the Manual installation window. Confirm the following settings before starting the installation.



- ① Select which manuals to install. The models that the manuals support are displayed in ② "Model List".
- ② The models that are supported by the manuals selected in ① are displayed here.
- ③ Select where to create the manuals shortcut icon when the manuals are installed.
- ④ Specify which folder on the PC to install the manuals to.
- ⑤ Click the [Install] button to start the installation.

Note

- To uninstall the manuals delete the shortcut icon from where you specified it to be installed (the default is on the desktop) during installation and the [Manual] folder from the folder (the default is C:\Panasonic) you specified during installation.

18.4 Installing the Viewer software

The Viewer software (Network Camera View 4S) must be installed on the PC in order to display unit images. On the CD launcher window, click the [Install] button next to [Viewer Software], and follow the instructions displayed on the window to install the software. A message is displayed if a PC that does not have the Viewer software installed tries to access the unit. Install the software by following the instructions displayed on the window. Refer to page 3 for further information.

Note

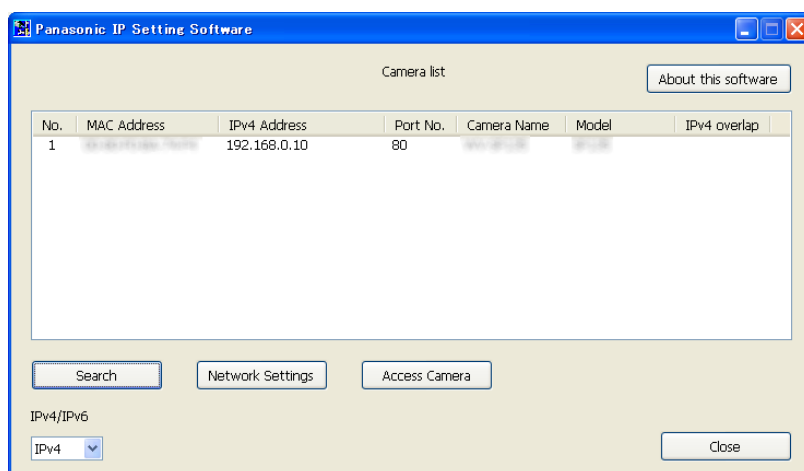
- To uninstall the Viewer software, follow the steps below depending on the OS used on your PC.
 - For Windows XP**
Delete [Network Camera View 4S] from [Control Panel] - [Add or Remove Programs].
 - For Windows Vista/Windows 7**
Delete [Network Camera View 4S] from [Control Panel] - [Programs] - [Uninstall a program].

18.5 Configure the network settings of the unit using the Panasonic “IP Setting Software”

It is possible to perform the network settings of the unit using the “IP Setting Software” on the provided CD-ROM. When using multiple units, it is necessary to configure the network settings of each unit independently. If the Panasonic “IP Setting Software” does not work, access the “Network” page from the setup menu of the unit in the browser and perform settings separately. (→page 66)

IMPORTANT

- When using Windows 7 or Windows Vista, the “Windows Security Alert” window may be displayed when starting the “IP Setting Software”. In this case, disable “User Account Control” from the control panel.
 - Panasonic “IP Setting Software” is inoperable in other subnets via the same router.
 - This unit cannot be displayed or set with an older version of the “IP Setting Software” (version 2.xx).
 - Due to security enhancements in “IP Setting Software”, “Network Settings” of the unit to be configured cannot be changed when around 20 minutes have passed after turning on the power of the unit. (When the effective period is set to “20min” in the “Easy IP Setup accommodate period”.) However, settings can be changed after 20 minutes for units in the initial set mode.
1. To start the Panasonic “IP Setting Software”, click the [Run] button next to [IP Setting Software] from the CD launcher menu window, or double-click on the shortcut icon created after installing the software on the PC.
 - The License Agreement will be displayed. Read the Agreement and choose “I accept the terms in the license agreement”, and click [OK].
 - The “IP Setting Software” screen is displayed. If a unit is found, information about it, such as the MAC address and IP address, is displayed.
 2. Click the [Access Camera] button after selecting the MAC address/IP address of the unit to be configured.



Note

- When using a DHCP server, the IP address assigned to the unit can be displayed by clicking the [Search] button of the “IP Setting Software”.
- When duplicate IP addresses are used, the number of the unit with the duplicate address is displayed in overlap.
- It is possible to change the “Camera list” display between IPv4 addresses and IPv6 addresses in accordance with the protocol in use.
- The information displayed can be sorted by clicking the title of each displayed item.

- When the [Network Settings] button is clicked, the “Network Settings” screen is displayed and network settings can be changed. For further information, refer to page 117.
3. The viewer software “Network Camera View 4S” must be installed in order to view images. Follow the on-screen instructions to install the software.
- The “Live” page of the unit is displayed.

Changing Network Settings

When changing settings related to the network settings, such as connection mode, IP address, and subnet mask, click the [Network Settings] button in [IP Setting Software] screen.

The “Network Settings” screen is displayed. Enter each item and then click the [Save] button.

Network Settings

Network Settings ☐ StaticIP ☐ DHCP
☐ Auto(AutoIP) ☒ Auto(Advanced)

Port No.

IPv4 Address

Subnet Mask

Default Gateway

DNS ☒ Auto ☐ Manual

Primary DNS

Secondary DNS

☒ Wait for camera restarting.

Note

- By unchecking the “Wait for camera restarting.” checkbox, multiple cameras can be continuously configured.
- For further information about each setting of the “Network Settings” page, refer to page 66.

IMPORTANT

- It may take for around 2 minutes to complete to upload the settings to the unit after clicking the [Save] button. The settings may be invalidated when the LAN cable is disconnected before completing the upload. In this case, perform the settings again.
- When using a firewall (including software), allow access to all UDP ports.

19 About the displayed system log

Error indications relating to SMTP

| Category | Indication | Description |
|-------------------|---|--|
| POP3 server error | Authentication error. | <ul style="list-style-type: none"> Entered user name or password may be incorrect. Check if the E-mail settings are configured correctly. |
| | Failed to find the POP3 server. | <ul style="list-style-type: none"> The IP address of the server may be incorrect. Check if the IP address of the server is configured correctly. The POP3 server may be down. Ask the network administrator. |
| SMTP server error | Authentication error. | <ul style="list-style-type: none"> Entered user name or password may be incorrect. Check if the E-mail settings are configured correctly. |
| | Failed to resolve the E-mail server address from DNS. | <ul style="list-style-type: none"> The designated IP address of the DNS may be incorrect. Check if the DNS settings are configured correctly. The DNS server may be down. Ask the network administrator. |
| | Failed to find the SMTP server. | <ul style="list-style-type: none"> The IP address of the server may be incorrect. Check if the IP address of the server is configured correctly. The SMTP server may be down. Ask the network administrator. |
| Internal error | Undefined error. | <ul style="list-style-type: none"> An error occurred in the E-mail function. Check if the E-mail settings are configured correctly. |

Error indications relating to FTP

| Category | Indication | Description |
|------------------|--|--|
| FTP server error | Failed to resolve the FTP server address from DNS. | <ul style="list-style-type: none"> The FTP server may be down. Ask the network administrator. |
| | Failed to find the FTP server. | <ul style="list-style-type: none"> The IP address of the server may be incorrect. Check if the IP address of the server is configured correctly. |
| Connection error | File transfer error. | <ul style="list-style-type: none"> The FTP server settings may be incorrect. Check if the FTP settings are configured correctly. The settings relating to the indicated item may be incorrect. Check if the FTP settings are configured correctly. |
| | Passive mode error. | |
| | Log out failed. | |
| | Failed to change the directory. | |
| | User name or password isn't correct. | |

| Category | Indication | Description |
|----------------|------------------|--|
| Internal error | Undefined error. | <ul style="list-style-type: none"> An error occurred in the FTP function. Check if the FTP settings are configured correctly. |

Error indications relating to “Viewnetcam.com”

| Category | Indication | Description |
|-----------------------------|---|--|
| Viewnetcam.com server error | Failed to resolve the Viewnetcam.com server address from DNS. | <ul style="list-style-type: none"> The designated IP address of the DNS may be incorrect. Check if the DNS settings are configured correctly. The DNS server may be down. Ask the network administrator. |
| Connection error | No response from the Viewnetcam.com server. | <ul style="list-style-type: none"> The “Viewnetcam.com” server may be down. Ask the network administrator. |
| | File transfer error. | |
| Internal error | Undefined error. | <ul style="list-style-type: none"> An error relating to the “Viewnetcam.com” function occurred. Check if the “Viewnetcam.com” settings are configured correctly. |

Error indications relating to Dynamic DNS Update

| Category | Indication | Description |
|-------------------|---|--|
| DDNS server error | Failed to resolve the DDNS server address from DNS. | <ul style="list-style-type: none"> The designated IP address of the DNS may be incorrect. Check if the DNS settings are configured correctly. The DNS server may be down. Ask the network administrator. |
| Connection error | No response from the DDNS server. | <ul style="list-style-type: none"> The DDNS server may be down. Ask the network administrator. |
| | Same host name has registered. | <ul style="list-style-type: none"> The same host name has already been registered in the DDNS server. Check if the DDNS Update settings are configured correctly. |
| Internal error | Undefined error. | <ul style="list-style-type: none"> An error occurred in the DDNS function. Check if the DDNS Update settings are configured correctly. |

Error indications relating to NTP

| Category | Indication | Description |
|-----------------------------------|----------------------------------|---|
| Connection error | No response from the NTP server. | <ul style="list-style-type: none"> The IP address of the server may be incorrect. Check if the IP address of the server is configured correctly. The NTP server may be down. Ask the network administrator. |
| Internal error | Undefined error. | <ul style="list-style-type: none"> An error occurred in the NTP function. Check if the NTP settings are configured correctly. |
| Synchronizing with NTP succeeded. | NTP update succeeded. | <ul style="list-style-type: none"> Time correction succeeded. |

Log indications relating to HTTPS

| Category | Indication | Description |
|----------|---|--|
| HTTPS | Self-signed Certificate - Generated | <ul style="list-style-type: none"> Generation of the self-signed certificate is complete. |
| | Self-signed Certificate - Deleted | <ul style="list-style-type: none"> Deletion of the self-signed certificate is complete. |
| | Certificate Signing Request - Generated | <ul style="list-style-type: none"> Generation of the CSR (Certificate Signing Request) is complete. |
| | CA Certificate - Installed | <ul style="list-style-type: none"> Installation of the server certificate is complete. |
| | CA Certificate - Deleted | <ul style="list-style-type: none"> Deletion of the server certificate is complete. |
| | Previous CRT key - Applied | <ul style="list-style-type: none"> Previous CRT key is applied. |
| | CRT key - Generated | <ul style="list-style-type: none"> Generation of the CRT key is complete. |

Log indications relating to login

| Category | Indication | Description |
|----------|-------------------------|---|
| Login | User name or IP address | <ul style="list-style-type: none"> The login user name will be displayed when "On" is selected for "User auth." The IP address of the PC currently accessing to the unit will be displayed when "On" is selected for "Host auth." |

Error indications relating to Panasonic alarm protocol notification

| Category | Indication | Description |
|---|--|---|
| Panasonic alarm protocol notification error | Failed to find destination of notification | <ul style="list-style-type: none">• The IP address of the destination of notification may be incorrect. Check if the IP address of the destination of notification is configured correctly.• The destination of notification may be down. Ask the network administrator. |
| | Cannot resolve notification addresses from DNS | <ul style="list-style-type: none">• The DNS server settings may be incorrect. Check if the DNS settings are configured correctly.• The DNS server may be down. Ask the network administrator. |

20 Troubleshooting

Before asking for repairs, check the symptoms with the following table.

Contact your dealer if a problem cannot be solved even after checking and trying the solution in the table or a problem is not described below.

| Symptom | Cause/solution | Reference pages |
|-------------------------------------|--|---------------------------|
| Cannot access from the web browser. | <ul style="list-style-type: none"> Is the power of the unit on? Check if the power of the unit is turned on. | Installation Guide |
| | <ul style="list-style-type: none"> Is the LAN cable (category 5 or better, straight, STP*) firmly connected to the network connector of the unit? *E model only | Installation Guide |
| | <ul style="list-style-type: none"> Is the live indicator lit? When it is not lit, connection to a LAN may not be established or a network may be not working correctly. Check if the cables have any contact failure or if the wiring is correct or not. | Installation Guide |
| | <ul style="list-style-type: none"> Are the set IP addresses valid? | 66 |
| | <ul style="list-style-type: none"> Are you accessing the wrong IP address? Check the connection as follows. With the Windows command prompt, > ping "IP address of the unit". If there is reply from the unit, the connection is normal. If there is no reply, check the connection with the following methods using a computer connected to the same network as the unit. If the firewall settings on the PC are enabled, temporarily disable them before performing settings on the unit. <ul style="list-style-type: none"> Start the Panasonic "IP Setting Software", confirm the unit's IP address, and then access that IP address. If the network settings (IP address, subnet mask, and default gateway) are incorrect, reboot the unit and change the network settings by using the Panasonic "IP Setting Software" within 20 minutes after the restart. In networks that do not have a DHCP server, the IP address of the unit will be configured to "192.168.0.10" when the unit is rebooted by holding the INITIAL SET button on the unit. After the unit is initialized, access the unit and set the IP address again. (When the unit is initialized, all the settings of the unit previously configured on the setup menus will be initialized.) | 116 Installation Guide |

| Symptom | Cause/solution | Reference pages |
|--|--|-----------------|
| | <ul style="list-style-type: none"> Is “554” selected for the HTTP port number? For the HTTP port number, select a port number other than the following port numbers used by the unit. The number used by the unit: 20, 21, 23, 25, 42, 53, 67, 68, 69, 110, 123, 161, 162, 443, 554, 995, 10669, 10670, 52000, 59000 - 61000 | 69 |
| Cannot access from the web browser. | <ul style="list-style-type: none"> Is the same IP address provided to other devices? Are there contradictions between the address and the network subnet to be accessed? When the unit and the PC are connected in the same subnet: Are the IP addresses of the unit and the PC set in a common subnet? Or is “Use Proxy Server” for the settings of the web browser checked? When accessing the unit in the same subnet, it is recommended to enter the address of the unit in the “Don’t Use Proxy For These Addresses” box. When the unit and the PC are connected in the different subnet: Is the IP address of the default gateway set for the unit correct? | - |
| | <ul style="list-style-type: none"> Is the name currently used to access the unit different from the name registered for the “Viewnetcam.com” service? Access the unit again with the registered name. | 93 |
| | <ul style="list-style-type: none"> Did you access “http://” while using the HTTPS function? To use the HTTPS function, access “https://”. It is also necessary to enter the port number. | 81 |
| Cannot access the unit via the Internet. | <ul style="list-style-type: none"> Are the network settings of the unit correct? Set the default gateway or DNS server address correctly. To use the DDNS service, check that the settings are correct. Is the setting for “Default gateway” on the “Network” page configured? Or is the setting correct? When communicating using IPv4: Configure the setting for “Default gateway” of “IPv4 network” on the [Network] tab of the setup menu. | 66 |

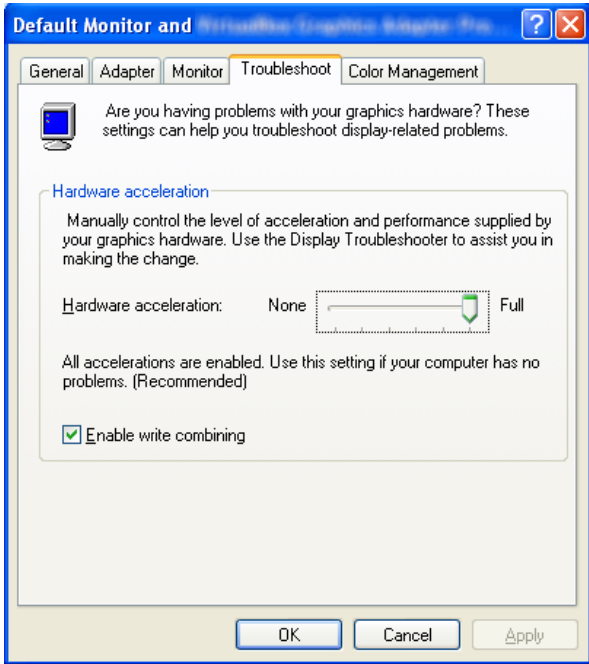
| Symptom | Cause/solution | Reference pages |
|---|--|-----------------|
| | <ul style="list-style-type: none"> Is the setting of port forwarding configured for the router? To enable the access to the unit via the Internet, it is necessary to perform the port forwarding setting when the router in use does not support the UPnP function. Refer to the manuals provided with the router for further information. Is UPnP function of the router disabled? Refer to the manuals provided with the router in use to enable the UPnP function. Is packet filtering set for the router to forbid the access via the Internet? Configure the settings of the router in use to enable the access via the Internet. Refer to the manuals provided with the router for further information about the settings. | 70 |
| | <ul style="list-style-type: none"> Are you accessing the unit using the local address (the IP address used in a local network)? When accessing the unit, use the global address (or the URL registered in the DDNS service) and the port number of the unit as the IP address to be used in the Internet. | 67 68 91 |
| Cannot access the unit via the URL of the "Viewnetcam.com" service. | <ul style="list-style-type: none"> Is the global address of unit (or router) notified to the "Viewnetcam.com" service server? Log into the "My Account" page of "Viewnetcam.com" website (http://www.viewnetcam.com/) to check the information of the registered unit. If the global address is not displayed for the IP address, access the unit, and register the user information for the "Viewnetcam.com" service on the [DDNS] tab on the "Network" page of the setup menu. In addition, check the "Status" of "Viewnetcam.com" (on the [Status] tab) and the system log (on the [System log] tab) of the "Maintenance" page of the setup menu. | 94 108 |
| Authentication window is displayed repeatedly. | <ul style="list-style-type: none"> Is the user name and password changed? While accessing the unit, when changing the user name and password of another user logging into the unit on another web browser, the authentication window will be displayed each time the screen is changed or refreshed. Have you changed the [Authentication] setting? When the [Authentication] setting has been changed, close the web browser, and then access the unit again. | - |
| It takes time to display the screen. | <ul style="list-style-type: none"> Are you accessing the unit in the HTTPS mode? In this mode, the refresh interval becomes slower due to decode procession. | - |

| Symptom | Cause/solution | Reference pages |
|--|---|-----------------|
| | <ul style="list-style-type: none"> Are you accessing another unit in the same local network via a proxy server? Configure the web browser to not use the proxy server. | - |
| | <ul style="list-style-type: none"> Are two or more users browsing the camera images simultaneously? It may take time to display the screen or refresh interval may become slower when two or more users browse the camera images simultaneously. | - |
| Cannot access the unit from a cellular phone. | <ul style="list-style-type: none"> Is the URL correct? Or is "/mobile" missing at the end of the URL? Check if the URL is entered correctly. When accessing the unit from a cellular phone, it is necessary to enter "/mobile" at the end of the URL that is used for the unit access from a PC. | 14 |
| | <ul style="list-style-type: none"> Is the SSL encryption method different from that of the unit? Select "HTTP" (Do not select "HTTPS") for "HTTPS" - "Connection" on the "Network" page - the [Network] tab, and access the unit again. | 71 |
| | <ul style="list-style-type: none"> Did you access "http://" while using the HTTPS function? To use the HTTPS function, access "https://". It is also necessary to enter the port number. | 81 |
| Cannot access the unit from a mobile terminal. | <ul style="list-style-type: none"> Is the URL correct? Or is "/cam" missing at the end of the URL? Check if the URL is entered correctly. When accessing the unit from a mobile terminal, it is necessary to enter "/cam" at the end of the URL that is used for the unit access from a PC. | 15 |
| | <ul style="list-style-type: none"> Is the SSL encryption method different from that of the unit? Select "HTTP" (Do not select "HTTPS") for "HTTPS" - "Connection" on the "Network" page - the [Network] tab, and access the unit again. | 71 |
| | <ul style="list-style-type: none"> Did you access "http://" while using the HTTPS function? To use the HTTPS function, access "https://". It is also necessary to enter the port number. | 81 |
| A cookie error was displayed when performing user registration for "Viewnetcam.com". | <ul style="list-style-type: none"> Is the web browser configured to allow cookies? Configure the web browser to allow cookies. In Internet Explorer, from [Tools] select [Internet Options] and configure the cookies setting in the [Privacy] tab. | - |

| Symptom | Cause/solution | Reference pages |
|--|---|--------------------|
| User registration for the "Viewnetcam.com" service fails. | <ul style="list-style-type: none"> Is the registered E-mail address correct? When an E-mail with the "Viewnetcam.com" website link is not received, the registered E-mail address may be incorrect. Visit the "Viewnetcam.com" website (http://www.viewnetcam.com/) to register the correct E-mail address. | - |
| No image is displayed. | <ul style="list-style-type: none"> Is the viewer software installed on the PC? Install the viewer software on a PC. | 3 |
| | <ul style="list-style-type: none"> Is the power of the connected camera turned on? Turn the power on for the connected camera. Is the BNC coaxial cable connected correctly to the video input? Check the video input connection. | Installation Guide |
| | <ul style="list-style-type: none"> Is the version of DirectX® 9.0c or later? Check the version of DirectX as follows. <ol style="list-style-type: none"> Select "Run..." from the start menu of Windows. Enter "dxdiag" in the displayed dialog box and click the [OK] button. If the version of DirectX is older than 9.0c, upgrade it. | - |
| | <ul style="list-style-type: none"> Is the cellular phone in use support the 320×240, 640×480, D1 (720×480) (NTSC), or D1 (720×576) (PAL) resolution? Or is the image data size too big to display images on the cellular phone? Refer to the manuals provided with the cellular phone in use for the restrictions of image data sizes. | - |
| No image is displayed. / Older images or logs are displayed. | <ul style="list-style-type: none"> When [Every time I visit the webpage] is not selected for [Check for newer versions of stored pages:] in the [Temporary Internet Files] section, images sometimes may not be displayed on the "Live" page. In this case, do the following. <ol style="list-style-type: none"> Select [Internet Options...] from [Tools] on the menu bar of Internet Explorer. The [Internet Options] window will be displayed. When using Internet Explorer 7.0, Internet Explorer 8.0, or Internet Explorer 9.0: Click the [Settings] button in the [Browsing history] section on the [General] tab, and then select [Every time I visit the webpage] for [Check for newer versions of stored pages:] in the [Temporary Internet Files] section on the [Temporary Internet Files and History Settings] window. When using Internet Explorer 6.0: Click the [Settings...] button in the [Temporary Internet Files] section on the [General] tab, and then select [Every visit to the page] for [Check for newer versions of stored pages:] on the [Settings] window. | - |

| Symptom | Cause/solution | Reference pages |
|---|--|--------------------|
| Images are not displayed correctly. | <ul style="list-style-type: none"> Do the video input settings (NTSC or PAL) of the connected camera match the "Video input" settings on the [JPEG/H.264] tab of the "Image" page? Change the "Video input" settings (NTSC or PAL) to match the settings of the camera. | 32 |
| Images are displayed blurry, not displayed (or too dark), or washed out. | <ul style="list-style-type: none"> Adjust the settings of the camera connected to the unit. | 9 40 |
| The image is not being refreshed. | <ul style="list-style-type: none"> Depending on the version of your browser, there might be difficulties refreshing the picture, etc. | Installation Guide |
| | <ul style="list-style-type: none"> Depending on the traffic of the network or the concentration of access to the unit, there might be difficulties displaying the camera picture. Request the camera picture using the web browser such as by pressing the [F5] key, etc. | - |
| The alarm occurrence indication button on the "Live" page do not display the current status in real time. | <ul style="list-style-type: none"> Is the viewer software installed on the PC? Confirm that the viewer software "Network Camera View 4S" is installed. | 3 |
| | <ul style="list-style-type: none"> Is "Real time" selected for "Alarm status update mode"? | 27 |
| No image is displayed on the "Live" page. | <ul style="list-style-type: none"> Press the [F5] key on the keyboard of the PC or click the [Live] button. | 9 |
| Shortcut icon of the unit is not displayed on "My Network Places" of the PC. | <ul style="list-style-type: none"> Is the Windows component of UPnP added? Add the component to the PC in use. | 70 |
| Images are not displayed or not refreshed smoothly. | <ul style="list-style-type: none"> Delete temporary internet files as follows. <ol style="list-style-type: none"> Select "Internet Options..." under "Tools" on the menu bar of Internet Explorer. The "Internet Options" window will be displayed. Click the [Delete Files...] button in the "Temporary Internet Files" section on the [General] tab. | - |
| | <ul style="list-style-type: none"> The firewall function of the anti-virus software may be filtering the port of the unit. Exclude the port number of the unit from the list of the port numbers to be filtered by the anti-virus software. | - |
| The live indicator is not lit. | <ul style="list-style-type: none"> Is "Off" selected for "Indicator" on the "Basic" page? Select "On" for "Indicator". | 27 |
| H.264 images are not displayed. | <ul style="list-style-type: none"> When "Network Camera View 4S" is deleted from a PC on which both the viewer software "Network Camera View 3" and "Network Camera View 4" are installed, H.264 images may not be displayed. In this case, delete "Network Camera View 3" from the PC and then install "Network Camera View 4S". | 3 |

| Symptom | Cause/solution | Reference pages |
|---|--|-----------------|
| Displayed images are distorted. | <ul style="list-style-type: none"> Images may be distorted when non-interlace signals, VCR (VTR) signals or signals not compliant with the standard in your locality are transmitted. | - |
| Black bars are displayed on both edges of the screen. | <ul style="list-style-type: none"> When the picture (camera) mode is D1, due to the standard of video signal, black bars appear instead of images on both edges of the screen. Black bar(s) also appear(s) even in the VGA mode when signals not compliant with the standard in your locality are transmitted. | - |
| The connected camera cannot be controlled. | <ul style="list-style-type: none"> Confirm that "On" is selected for "RS485 transmission" on the [RS485] tab. Confirm that each of the settings on the [RS485] tab match the settings of the connected camera. If Pan/Tilt/Zoom functions cannot be operated for Panasonic cameras, you must select "Custom" for "Protocol" on the [RS485] tab of the "Image" page and upload the command table to the unit. For further information, refer to our website (http://panasonic.net/pss/security/support/info.html). | 41 |

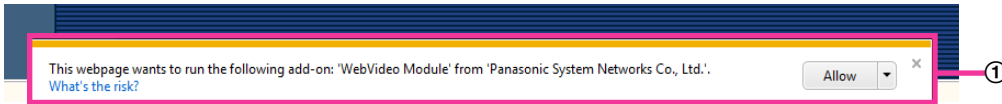
| Symptom | Cause/solution | Reference pages |
|---|--|-----------------|
| <p>When displaying H.264 images on two or more web browser windows, images from two or more cameras are displayed in sequence on a single browser window.</p> | <ul style="list-style-type: none"> This may occur due to the display adapter and driver combination. When this has occurred, first update the driver of the display adapter to the latest version. If updating the driver does not solve the problem, adjust the hardware acceleration as follows. The following are descriptions for when Windows XP is installed on the PC in use. <ol style="list-style-type: none"> Right-click on the desktop and select "Properties" from the displayed pop-up menu. Select "Settings" from "Display Properties", and then click the [Advanced] button. Click the [Troubleshoot] tab and disable the DirectDraw acceleration by adjusting the level of Hardware acceleration.  | - |

Information Bar

Depending on the OS installed on the PC, the following may occur. Follow the instructions below when the following has occurred. By performing the following solutions, other applications may not be affected.

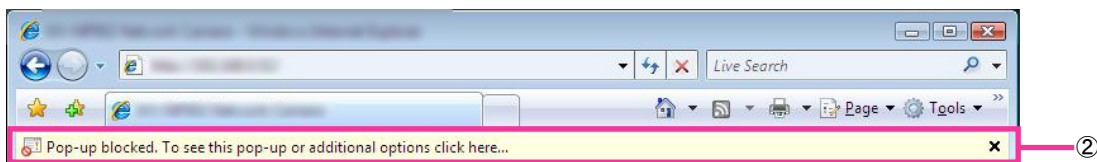
When using Internet Explorer 9.0:

The “Information Bar” (①) expressed in the following symptom and solutions will be displayed just below the address bar only when there is information to communicate.



When using Internet Explorer 6.0, Internet Explorer 7.0, or Internet Explorer 8.0:

The “Information Bar” (②) expressed in the following symptom and solutions will be displayed just below the address bar only when there is information to communicate.



| Symptom | Cause/solution | Reference pages |
|---|---|-----------------|
| The following message is displayed on the information bar. “Pop-up blocked. To see this pop-up or additional options, click here...” (Internet Explorer 6, Internet Explorer 7, or Internet Explorer 8) | <ul style="list-style-type: none"> Click the information bar and select “Always Allow Pop-ups from This Site...”. The dialog window saying “Allow pop-ups from this site?” will be displayed. Click the [Yes] button. | - |
| The following message is displayed on the information bar. “This webpage wants to run the following add-on: `WebVideo Module' from `Panasonic System Networks Co.,Ltd.`.” (Internet Explorer 9) | <ul style="list-style-type: none"> Select [Allow]. | - |
| The following message is displayed on the information bar. “This site might require the following ActiveX control 'nwc4Ssetup.exe' from 'Panasonic System Networks Co.,Ltd.'. Click here to install...” (Internet Explorer 6, Internet Explorer 7, or Internet Explorer 8) | <ul style="list-style-type: none"> Click the information bar and select “Install ActiveX Control”. The “Security Warning” window will be displayed. Click the [Install] button on the displayed “Security Warning” window. | - |

| Symptom | Cause/solution | Reference pages |
|--|--|-----------------|
| The following message is displayed on the information bar. "This webpage wants to install the following add-on: `nwc4Ssetup.exe' from `Panasonic System Networks Co.,Ltd.'" (Internet Explorer 9) | <ul style="list-style-type: none"> Select [Install]. The "Security Warning" window will be displayed. Click the [Install] button on the displayed "Security Warning" window. | - |
| An unnecessary status bar or scroll bar is displayed on the pop-up window. | <ul style="list-style-type: none"> Click "Internet Options..." under "Tools" of the menu bar of Internet Explorer, and then click the [Security] tab. Click "Internet" in the "Select a Web content zone to specify its security settings:" section. Then, click the [Custom Level...] button to open the "Security Setting" window. Under "Miscellaneous", select "Enable" for "Allow script-initiated windows without size or position constraints". Click the [OK] button. When the warning window is displayed, click the [Yes] button. | - |
| Images are not fit in the frames. | <ul style="list-style-type: none"> When "120 DPI" is selected for "DPI setting", they may not be displayed correctly. Click the "Settings" tab on the "Properties" window of "Screen" (in the control panel), and then click the [Advanced] button. Change the "DPI setting" as necessary. | - |

For U.S. and Canada:

**Panasonic System Communications Company of North America,
Unit of Panasonic Corporation of North America**

www.panasonic.com/business/

For customer support, call 1.800.528.6747

Three Panasonic Way, Secaucus, New Jersey 07094 U.S.A.

Panasonic Canada Inc.

5770 Ambler Drive, Mississauga, Ontario, L4W 2T3 Canada

(905)624-5010

www.panasonic.ca

For Europe and other countries:

Panasonic Corporation

<http://panasonic.net>

Importer's name and address to follow EU rules:

Panasonic Testing Centre

Panasonic Marketing Europe GmbH

Winsbergring 15, 22525 Hamburg, Germany